PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-055961
(43)Date of publication of application : 20.02.2002

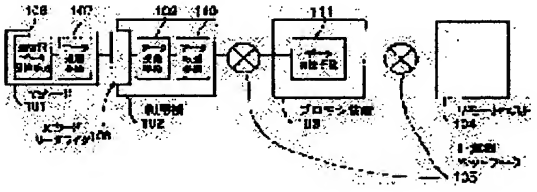
(51)Int.CI. G06F 15/00
B42D 15/10
G06K 17/00
G06K 19/07
G09C 1/00

(21)Application number : 2000-245818
(22)Date of filing : 14.08.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : INOUE KAZUNORI
SAKUSHIMA KAZUO
TANABIKI MASAKI
KIKUCHI TAKAFUMI

(54) IC CARD DEVICE AND PROXY DEVICE, AND CARD TERMINAL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To allow an IC card system to make access destination information, etc., secret to a used machine and also prevent the secret information from leaking from the used machine when the security of the used machine is not high enough.
SOLUTION: This IC card system is equipped with an IC card 101, the used machine 102 which is connected by a computer network 105, a proxy device 103, and a remote host 104. When network service is received by accessing the remote host 104 by using the IC card 101, the IC card 101 and proxy device 103 communicate with each other. At this time, an application program on the IC card 101 and a data converting means 111 of the proxy device 103 settle a rule and a method for data conversion and the used machine 102 performs data conversion by unknown conversion algorithm to send and receive data. Consequently, information can be kept secret to the used machine 102 and its disclosure can be limited.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－55961
（P2002－55961A）
(43)公開日　平成14年２月20日(2002.2.20)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ　２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１　５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｄ　５Ｂ０５８
19/07		Ｇ０９Ｃ　1/00	６６０Ａ　５Ｂ０８５
Ｇ０９Ｃ　1/00	６６０	Ｇ０６Ｋ　19/00	Ｎ　５Ｊ１０４

審査請求　未請求　請求項の数64　ＯＬ　（全 44 頁）

(21)出願番号　特願2000－245818(P2000－245818)

(22)出願日　平成12年８月14日(2000.8.14)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　井上　和紀
大阪府門真市大字門真1006番地　松下電器産業株式会社内

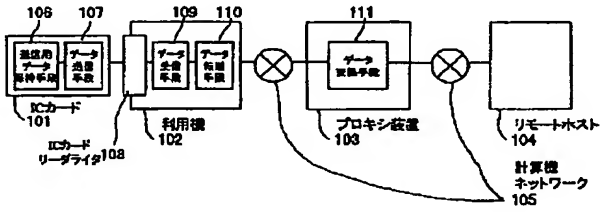
(72)発明者　佐久嶋　和生
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100105647
弁理士　小栗　昌平　（外４名）

最終頁に続く

(54)【発明の名称】　ＩＣカード装置及びプロキシ装置、並びにカード端末装置

(57)【要約】
【課題】　ＩＣカードシステムにおいて、利用機のセキュリティが充分強固でない場合にアクセス先情報等を利用機に対して秘匿したり利用機からの機密情報漏洩を防止する。
【解決手段】　ＩＣカードシステムは、ＩＣカード１０１と、計算機ネットワーク１０５で接続された利用機１０２、プロキシ装置１０３、リモートホスト１０４とを備える。ＩＣカード１０１を用いてリモートホスト１０４にアクセスしてネットワークサービスを受ける際、ＩＣカード１０１とプロキシ装置１０３とで通信を行う。このとき、予めＩＣカード１０１内のアプリケーションプログラムとプロキシ装置１０３のデータ変換手段１１１との間でデータ変換の規則と方法についての取り決めを行い、利用機１０２において未知の変換アルゴリズムでデータ変換を行ってデータをやり取りする。これにより、利用機１０２に対して情報の秘匿や開示制限を行う。



1

【特許請求の範囲】

【請求項１】　半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、
送信用のデータを保持する送信用データ保持手段と、
前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段とを備え、
前記カード端末装置と計算機ネットワークを介して接続されたリモートホストとデータ通信を行う際に、このリモートホストと前記カード端末装置との間に設けられるプロキシ装置と当該ＩＣカード装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するためのデータを前記プロキシ装置へ送信することを特徴とするＩＣカード装置。

【請求項２】　前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を、前記カード端末装置が解釈困難なキーデータとして生成する通信キーデータ生成手段を備え、
前記変換アルゴリズムもしくは変換パラメータとして、当該ＩＣカード装置と前記プロキシ装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いてデータ変換処理を実行する際に、前記通信キーデータを前記プロキシ装置へ送信することを特徴とする請求項１記載のＩＣカード装置。

【請求項３】　通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記プロキシ装置または前記リモートホストとの間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成することを特徴とする請求項１記載のＩＣカード装置。

【請求項４】　前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記プロキシ装置との間で形成したセキュアパスを経由して該プロキシ装置へ送ることを特徴とする請求項３記載のＩＣカード装置。

【請求項５】　前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第２の暗号処理手段を備え、
前記第２の暗号処理手段により当該ＩＣカード装置が保持する任意のデータを暗号化し、この第２の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第２の暗号化データを前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送ることを特徴とする請求項４記載のＩＣカード装置。

【請求項６】　前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順

2

を異なる鍵情報を用いることによりデータの暗号化を行う第２の暗号処理手段を備え、
前記第２の暗号処理手段により当該ＩＣカード装置が保持する任意のデータを暗号化し、この第２の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第２の暗号化データを前記リモートホストのアクセス先情報の暗号化データと共に前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送ることを特徴とする請求項４記載のＩＣカード装置。

【請求項７】　当該ＩＣカード装置と前記プロキシ装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項３～６のいずれかに記載のＩＣカード装置。

【請求項８】　当該ＩＣカード装置と前記プロキシ装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項３～６のいずれかに記載のＩＣカード装置。

【請求項９】　半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、
送信用のデータを保持する送信用データ保持手段と、
前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、
前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を、このカード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置に送信するＵＩリクエスト情報送信手段とを備えたことを特徴とするＩＣカード装置。

【請求項１０】　前記ＵＩリクエスト情報として、文字コードに関わる文字列情報を用いることを特徴とする請求項９記載のＩＣカード装置。

【請求項１１】　前記ＵＩリクエスト情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させるためのプログラム情報による動作結果に影響を与えるパラメータ情報を用いることを特徴とする請求項９記載のＩＣカード装置。

【請求項１２】　半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、
送信用のデータを保持する送信用データ保持手段と、
前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、
前記カード端末装置の認証を行う端末認証手段と、
前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、
データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、
前記カード端末装置が接続された計算機ネットワーク上

において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記プロキシ装置へ送ることを特徴とするＩＣカード装置。

【請求項１３】　半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、

送信用のデータを保持する送信用データ保持手段と、

前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、

データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、

前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記プロキシ装置から前記カード端末装置の信頼度評価結果を受け取ることを特徴とするＩＣカード装置。

【請求項１４】　前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えることを特徴とする請求項１２または１３に記載のＩＣカード装置。

【請求項１５】　前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してＩＣカード装置から送信する情報の一部もしくは全てを削除もしくは変更することを特徴とする請求項１４記載のＩＣカード装置。

【請求項１６】　前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持する機密情報に関わる情報を削除もしくは変更することを特徴とする請求項１５記載のＩＣカード装置。

【請求項１７】　前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持するＩＣカードユーザのプライバシに関わる情報を削除もしくは変更することを特徴とする請求項１５記載のＩＣカード装置。

【請求項１８】　半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、

送信用のデータを保持する送信用データ保持手段と、

前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、

前記カード端末装置と計算機ネットワークを介して接続されたリモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段とを備え、

前記機密情報変換手段は前記カード端末装置より入力された第１の機密情報データを当該カード端末装置に対して秘匿性を持った第２の機密情報データに変換し、この第２の機密情報データを前記カード端末装置と前記リモートホストとの間に設けられるプロキシ装置へ送ることを特徴とするＩＣカード装置。

【請求項１９】　前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてＩＣカードユーザに提示し、前記カード端末装置より入力された第１の機密情報データから前記変換キーデータを用いて前記第２の機密情報データを生成することを特徴とする請求項１８記載のＩＣカード装置。

【請求項２０】　前記変換キーデータと前記第１の機密情報データとを一対一に対応させて同一の第２の機密情報データを生成するための異なるデータの組を複数設けたことを特徴とする請求項１９記載のＩＣカード装置。

【請求項２１】　前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を前記プロキシ装置に送信するＵＩリクエスト情報送信手段を備え、

前記ＵＩリクエスト情報として、前記リモートホストから要求される機密情報として前記第２の機密情報データの代わりに前記第１の機密情報データを入力すべきことをＩＣカードユーザに指示するためのＵＩ部品情報を用いることを特徴とする請求項１８～２０のいずれかに記載のＩＣカード装置。

【請求項２２】　予め定めた規則に従って計算機ネットワーク上の複数のプロキシ装置の中から一つを選択するプロキシ選択手段を備えたことを特徴とする請求項１～２１のいずれかに記載のＩＣカード装置。

【請求項２３】　前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置を逐次的に検索して選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２４】　前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置をランダムに検索して選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２５】　前記プロキシ選択手段は、前記カード端末装置に問い合わせて使用に適するプロキシ装置を選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２６】　使用に適するプロキシ装置を選択するためのプロキシ装置のリストを有し、このリスト内容の追加、変更、削除の少なくともいずれか一つを行うプロキシ情報操作手段を備えたことを特徴とする請求項２２記載のＩＣカード装置。

【請求項２７】　前記カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態

を電子情報のやりとりによって生じさせるインセンティブを発行するインセンティブ発行手段を備え、このインセンティブに関する情報を前記カード端末装置との間で通信することを特徴とする請求項１～２６のいずれかに記載のＩＣカード装置。

【請求項２８】　前記インセンティブとして広告情報を用い、前記インセンティブ発行手段は前記カード端末装置からこの広告情報を受信することを特徴とする請求項２７記載のＩＣカード装置。

【請求項２９】　前記インセンティブとして金銭あるいは有価値物に関連した有価値電子情報を用い、前記インセンティブ発行手段はこの有価値電子情報を前記カード端末装置に送信することを特徴とする請求項２７記載のＩＣカード装置。

【請求項３０】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、

前記ＩＣカード装置と当該プロキシ装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するデータ変換手段を備えたことを特徴とするプロキシ装置。

【請求項３１】　前記データ変換手段は、前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を前記カード端末装置が解釈困難なキーデータとして生成した通信キーデータを変換するもので、前記変換アルゴリズムもしくは変換パラメータとして、当該プロキシ装置と前記ＩＣカード装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いて変換処理を行うことを特徴とする請求項３０記載のプロキシ装置。

【請求項３２】　通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成することを特徴とする請求項３０記載のプロキシ装置。

【請求項３３】　前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記ＩＣカード装置との間で形成したセキュアパスを経由して該ＩＣカード装置から受け取ることを特徴とする請求項３２記載のプロキシ装置。

【請求項３４】　当該プロキシ装置と前記ＩＣカード装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項３２または３３に記載のプロキシ装置。

【請求項３５】　当該プロキシ装置と前記ＩＣカード装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項３２または３３に記載のプロキシ装置。

【請求項３６】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、

前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を受信するＵＩリクエスト情報受信手段と、

前記受信したＵＩリクエスト情報の内容に基づいて前記カード端末装置におけるユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段とを備えたことを特徴とするプロキシ装置。

【請求項３７】　前記ＵＩ情報として、文字フォントに関わる文字画像情報を用いることを特徴とする請求項３６記載のプロキシ装置。

【請求項３８】　前記ＵＩ情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いることを特徴とする請求項３６記載のプロキシ装置。

【請求項３９】　前記ＵＩ情報として、前記カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いることを特徴とする請求項３８記載のプロキシ装置。

【請求項４０】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、

前記カード端末装置の認証を行う端末認証手段と、

前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、

データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、

前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記ＩＣカード装置へ送ることを特徴とするプロキシ装置。

【請求項４１】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、

データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、

前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記ＩＣカード装置から前記カード端末装置の信頼度評価結果を受け取ることを特徴とするプロキシ装置。

【請求項４２】　前記端末認証手段と前記端末信頼度評価手段の少なくとも一方が、前記カード端末装置の計算機ネットワークへの接続に関わる固有かつ一意の情報を用いて動作することを特徴とする請求項４０記載のプロキシ装置。

【請求項４３】　前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えることを特徴とする請求項４０または４１に記載のプロキシ装置。

【請求項４４】　前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置から送信する情報の一部もしくは全てを削除もしくは変更することを特徴とする請求項４３記載のプロキシ装置。

【請求項４５】　前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する機密情報に関わる情報を削除もしくは変更することを特徴とする請求項４４記載のプロキシ装置。

【請求項４６】　前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持するＩＣカードユーザまたはプロキシユーザのプライバシに関わる情報を削除もしくは変更することを特徴とする請求項４４記載のプロキシ装置。

【請求項４７】　前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段を備え、
前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置からＵＩ情報を送信する前に、前記ＵＩ情報の中から機密情報表示に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のＵＩ情報を前記カード端末装置へ送ることを特徴とする請求項４４記載のプロキシ装置。

【請求項４８】　前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段を備え、
前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置からＵＩ情報を送信する前に、前記ＵＩ情報の中から機密情報入力に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のＵＩ情報を前記カード端末装置へ送ることを特徴とする請求項４４記載のプロキシ装置。

【請求項４９】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、
前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段を備え、
前記機密情報変換手段は前記カード端末装置より入力された第１の機密情報データを当該カード端末装置に対して秘匿性を持った第２の機密情報データに変換し、この第２の機密情報データを前記リモートホストへ送ることを特徴とするプロキシ装置。

【請求項５０】　ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、
前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報に関して、前記カード端末装置より入力された第１の機密情報データが当該カード端末装置に対して秘匿性を持った状態に変換された第２の機密情報データを、前記ＩＣカード装置から受け取って前記リモートホストへ送る機密情報獲得手段を備えたことを特徴とするプロキシ装置。

【請求項５１】　前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてＩＣカードユーザに提示し、前記カード端末装置より入力された第１の機密情報データから前記変換キーデータを用いて前記第２の機密情報データを生成することを特徴とする請求項４９記載のプロキシ装置。

【請求項５２】　前記変換キーデータと前記第１の機密情報データとを一対一に対応させて同一の第２の機密情報データを生成するための異なるデータの組を複数設けたことを特徴とする請求項５１記載のプロキシ装置。

【請求項５３】　前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段を備え、
前記ＵＩ情報として、前記リモートホストから要求される機密情報として前記第２の機密情報データの代わりに前記第１の機密情報データを入力すべきことをＩＣカードユーザに指示するためのＵＩ部品情報を用いることを特徴とする請求項４９～５２のいずれかに記載のプロキシ装置。

【請求項５４】　ＩＣカード装置とデータのやり取りを行うＩＣカードシステム用のカード端末装置であって、
当該カード端末装置は計算機ネットワーク上において設けられるプロキシ装置と接続され、
前記プロキシ装置から送られた当該カード端末装置におけるユーザインタフェース部品に関わるＵＩ情報を受信するＵＩ情報受信手段と、
前記受信したＵＩ情報の内容に基づいて前記ＩＣカード装置とのデータ通信に関するユーザインタフェースを実

行するＵＩ実行手段とを備えたことを特徴とするカード端末装置。

【請求項５５】　前記ＵＩ情報として、文字フォントに関わる文字画像情報を用いることを特徴とする請求項５４記載のカード端末装置。

【請求項５６】　前記ＵＩ情報として、当該カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いることを特徴とする請求項５４記載のカード端末装置。

【請求項５７】　前記ＵＩ情報として、当該カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いることを特徴とする請求項５６記載のカード端末装置。

【請求項５８】　ＩＣカード装置とデータのやり取りを行うＩＣカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上において設けられる複数のプロキシ装置と接続され、
前記ＩＣカード装置からの問い合わせに応じて、予め定めた規則に従って使用に適するプロキシ装置を選択するための処理を行うプロキシ選択処理手段を備えたことを特徴とするカード端末装置。

【請求項５９】　当該カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを受けるインセンティブ獲得手段を備え、このインセンティブに関する情報を前記ＩＣカード装置との間で通信することを特徴とする請求項５４～５８のいずれかに記載のカード端末装置。

【請求項６０】　前記インセンティブとして広告情報を用い、前記インセンティブ獲得手段はこの広告情報を前記ＩＣカード装置に送信することを特徴とする請求項５９記載のカード端末装置。

【請求項６１】　前記インセンティブとして金銭あるいは有価値物に関連した有価値電子情報を用い、前記インセンティブ獲得手段は前記ＩＣカード装置からこの有価値電子情報を受信することを特徴とする請求項５９記載のカード端末装置。

【請求項６２】　請求項１～２９のいずれかに記載のＩＣカードシステム用のＩＣカード装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【請求項６３】　請求項３０～５３のいずれかに記載のＩＣカードシステム用のプロキシ装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【請求項６４】　請求項５４～６１のいずれかに記載のＩＣカードシステム用のカード端末装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカードシステムを構成するのに好適なカード本体を含むＩＣカード装置、及びこのＩＣカードと接触又は非接触でデータ通信を行うカード端末装置、並びにこのカード端末装置とネットワークを介して接続されるリモートホストとの間に設けてＩＣカード装置とリモートホストの両者に対してデータ通信を行うプロキシ装置に関する。

【０００２】

【従来の技術】一般に知られるＩＣカードシステムは、図３５に示すように、半導体記憶媒体を含むカード本体であるＩＣカード５１、カード端末装置である利用機（ＩＣカード利用機）５２、利用機５２に対して情報の提供等を行うリモートホスト（ホストコンピュータ）５３から構成される。利用機５２は、リーダライタ５５と端末５６からなり、端末５６はリーダライタ５５を介してＩＣカード５１とデータ送受信を行う。さらに、端末５６はネットワーク５４を介してリモートホスト５３ともデータ送受信を行う。リーダライタ５５は、ＩＣカード５１に対し電源、クロックを提供するが、その際、接触端子を用いて電気的に伝達する方法と、電磁波を用いて伝達する方法とがあり、それぞれ接触型、非接触型と呼ばれる。ＩＣカード５１それ自体は通常はユーザインタフェースを持たず、暗証入力、処理選択、表示等の機能は利用機５２が担う。

【０００３】ＩＣカードの利点は、ＩＣカードに内蔵されるＩＣチップの対タンパ性（物理的、化学的、電気的手段等によりＩＣチップ内部状態の解析や改竄を試みる不正行為からＩＣチップ内部の情報を保護する能力）に優れることである。さらに、ＩＣカードの中でマイコンカードに分類されるものの多くは、ＩＣチップ内で暗号処理（データを暗号アルゴリズムと鍵を用いて解読困難な状態に変換する処理）が可能となっており、電子商取引等の高いセキュリティが求められる分野での利用に適する。

【０００４】計算機ネットワークにおいて暗号処理機能を有するＩＣカードを利用する技術は、特開平４－３５５３８号公報（暗号化通信方式、以下従来例１とする）、特開平４－３２６４４２号公報（メッセージ認証システム、従来例２）、特開平５－１１０８７３号公報（暗号機能通信システム、従来例３）に示されている。これらはいずれも計算機ネットワークに接続された利用機にＩＣカードを接続し、ＩＣカードが内部にもつ暗号処理機能を用いてネットワーク上で送受するデータの秘匿及び認証を行うものである。

【０００５】ＩＣカードのもう一つ利点は可搬性の高さである。この性質を利用し、ユーザ自身の固有情報を格納したＩＣカードを訪問先の端末で使用する技術は、特開平７－３０６８３１号公報（コンピュータネットワー

クシステム、従来例４）、特開平１０－２１３０１号公報（地域保険医療情報システム及びこれに用いる可搬型記憶媒体、従来例５）、特開平１１－１５９２７号公報（ＩＣカードシステム、従来例６）に示されている。これらの技術によれば、計算機ネットワーク上の複数の場所から共通のユーザ環境を得たり、一貫したサービスを受けたりすることができる。

【０００６】また近年では、ＩＣカードに内蔵されるＩＣチップの性能の向上（処理速度、記憶容量の向上）とソフトウェア技術の向上（マルチアプリケーション環境の実現、仮想マシンによるソフトウェア不正動作の防止、カード発行後のアプリケーションダウンロード等）に伴い、より高機能、多用途、複雑なアプリケーションプログラムをＩＣカード上で動作させることが可能になっている。

【０００７】

【発明が解決しようとする課題】従来の多くのＩＣカードシステムは、基本的に利用機が主、ＩＣカードが従の関係にあり、ＩＣカードは情報記憶媒体的な使われ方をされることがほとんどであったが、今後はＩＣカード内に記憶されたアプリケーションプログラムが主体となってネットワーク上のサービスを受けるシステムが普及することが予想される。

【０００８】例えば、ＩＣカード内のアプリケーションプログラムが、ＩＣカード内に格納されたアクセス情報から計算機ネットワーク上のどのリモートホストに、どのような手順でアクセスするかを判断し、同じくＩＣカード内に格納されたデータ情報をリモートホストに送信する、もしくはリモートホストからデータ情報を取得してＩＣカード内に格納する、といったシステムである。

【０００９】より具体的な例として次のようなＩＣカードシステムを考える。インターネットに代表される大規模計算機ネットワーク空間で、WWW（World Wide Web）に代表される仕組みを用いて多種のサービスが、それぞれ別個のリモートホスト（サーバサイト）によって運営されている。さらに、駅、店舗、公共施設等の、不特定多数の人間が訪れる場所に利用機を設置する。利用機の適例はキオスク端末である。キオスク端末は、不特定多数のユーザに情報提示や各種のサービスを行うことを目的とした計算機であり、ここではディスプレイ、プリンタ、タッチパネル、キーパッド等のユーザインタフェース、ネットワークインタフェース、ＩＣカードリーダライタを持つものを想定する。

【００１０】ユーザは、上記の利用機を用いてネットワーク上のサービスを利用するためのＩＣカードを個々に所持し、行く先々に設置された任意の利用機にＩＣカードを接続することで、それらのサービスを受けることができる。

【００１１】サービスを受けるためのクライアントソフトウェアは、ＩＣカード内にアプリケーションとして格納される。即ち、どのようなアプリケーションをＩＣカード内に持たせるかによって、ユーザが受けられるサービス内容が変わる。これはパーソナルコンピュータやワークステーションを用いてインターネット上のサービスを受ける場合と類似しており、原理的にはＩＣカード内にWWWブラウザや電子メールクライアントを持たせることも可能である。

【００１２】ＩＣカード内にWWWブラウザを持たせた場合、ユーザはそのＩＣカードを用いてインターネット上のウェブコンテンツ（WWWによって公開されるマルチメディア情報）を閲覧できる他、ウェブメール（WWWの仕組みを利用した個人向け電子メールサービス）、電子掲示板、オンラインショッピング等のサービスを受けられる。これにより、ユーザは携帯型コンピュータ等を持ち運ばなくとも、上記のＩＣカードを１枚持ち歩くだけで、訪問先にある利用機からこれらのサービスを受けることが可能となる。これは、例えば携帯電話機のような小型通信情報機器を利用する場合と比較しても、画面解像度を始めとしたユーザインタフェースの品質、通信品質、ユーザ負担コスト等の面で優位性があるものと考えられる。

【００１３】しかしながら、このようなＩＣカードシステムを従来技術で実現しようとした場合、次のような問題が生じる。

【００１４】第１に、ＩＣカード内のアプリケーションによってユーザがアクセスしたネットワーク上のリモートホストの位置（インターネットであればホスト名、ドメイン名及びＩＰアドレス）が、利用機に掌握されてしまう。これは、ＩＣカードそれ自体が利用機のＩＣカードリーダライタとの間の低レベルな通信（一般的にはシリアル通信）機能しか持たず、ネットワーク通信の全てを利用機に依存していることに起因する。前記の従来例１～３に示される暗号応用技術によって、ＩＣカードとリモートホストの間で交された通信内容は利用機に対し秘匿することが可能であるが、利用機からリモートホストへ直接ネットワーク通信のコネクションを張っている限り、アクセス先がどのホストであったのかを隠すことはできない。アクセス先が特定できると、そのユーザが受けたサービスの種類や性質を推定されることも有り得る（例：コンピュータゲームの通信販売サイトへアクセスしたユーザは、少なくともコンピュータゲームに興味があり、もしかしたらそのサイトで何か商品を購入した可能性もある、等）。ユーザのプライバシ保護の観点からはアクセス先情報の漏洩は好ましいことではない。

【００１５】第２に、ＩＣカード内のアプリケーションがユーザに提示した出力の内容、及びＩＣカード内のアプリケーションに対してユーザが行った入力の内容が、全て利用機に掌握されてしまう。これは上記と同様、一般にＩＣカードそれ自体がユーザインタフェースを持たず、全て利用機を介してユーザとのインタラクションを

行うことに起因する。具体的には、利用機の画面に表示あるいはプリンタにて印刷した出力内容は、それが文字であっても画像であっても、原理的に全て利用機がコピーを取得し、保存したり他に転用したりすることが可能である。また、ユーザからの入力についても同様であり、例えばアカウント情報やパスワード情報、クレジットカード番号等を利用機から直接入力した場合、それらの内容を利用機に対して秘匿することは不可能である。前記の従来例１～５に示した技術において、このような問題は考慮されていない。

【００１６】ＩＣカードのユーザが、利用機の運用者、運用ポリシ、悪意のある第三者に対するセキュリティ強度について充分納得し、利用機を信用できる場合には、上記のようなことは問題にならないが、そうでない場合ＩＣカードユーザは利用機を安心して使うことができない。

【００１７】逆の見方をすると、従来は利用機を設置する場合、ＩＣカードユーザ、及びリモートホスト運用者に対してセキュリティ上の保証をする必要があり、そのためにハードウェアの不正使用の防止対策、ネットワークからの不正行為対策に加え、運用母体と運用ポリシを明確にし、設置した利用機が不正なもの、危険なものでないことを証明してオーソライズされる必要があった。これはハードウェア価格や運営コスト高騰の問題として顕在化する可能性が極めて高く、利用機普及の阻害要因となり、結果的にＩＣカードユーザが得るメリットも小さくなってしまう。

【００１８】本発明は上記のような問題点を解決するものであり、オーソライズ不要の安価なカード端末設置を可能とし、またＩＣカードユーザにとっては信頼度の低い、もしくは信頼度のはっきりしないカード端末装置を用いた場合でも、プライバシや財産に関わる個人の機密情報を漏らすことなく、安全が保証できる範囲でのネットワーク利用が可能になる、セキュアかつ利便性の高いＩＣカードシステムを構築可能なＩＣカード装置及びプロキシ装置、並びにカード端末装置を提供することを目的とする。

【００１９】

【課題を解決するための手段】上記の課題を解決するため本発明は、第１に、ＩＣカード装置（ＩＣカード）や通信相手先のリモートホストの代理として計算機ネットワーク上で代理装置などとして機能するプロキシ装置を設ける。プロキシ装置はネットワーク通信手段を持ち、カード端末装置（利用機）とリモートホストの両者と通信を行う。さらに、プロキシ装置にデータ変換手段を設け、ＩＣカード装置からカード端末装置経由で受信したデータを、ＩＣカード装置が既知かつカード端末装置が未知の変換アルゴリズムもしくはパラメータを用いてデータ変換を行う。ＩＣカード装置には、送信用データ保持手段と、これに保持されているデータをカード端末装置に送信するデータ送信手段とを設ける。カード端末装置には、ＩＣカード装置からデータを受信するデータ受信手段と、データ受信手段が得たデータをプロキシ装置に送信するデータ転送手段とを設ける。これにより、ＩＣカード装置がプロキシ装置に渡したデータは、ＩＣカードユーザの意図通りに、かつカード端末装置のユーザにその内容を知られることなく、プロキシ装置内部において異なるデータに変化させることが可能となる。

【００２０】第２に、上記の送信用データとして、ＩＣカード装置内のアプリケーションがアクセスしようとするホストのネットワーク上の位置及び通信方法を得るための情報を準備する通信キーデータ生成手段を設ける。通信キーデータは、ＩＣカード装置内のメモリに書かれたデータと同一のものを用いても構わないし、ＩＣカード装置内部で変換処理を行った結果を用いても構わない。ただし、通信キーデータそのものからカード端末装置が容易にアクセス先を特定できないこと、さらに、プロキシ装置は受け取った通信キーデータ及び予めプロキシ装置内部に持つプログラムとデータにより、アクセス先を特定できることの２点が条件となる。予めＩＣカード装置とプロキシ装置の二者で取り決めた、通信キーデータからアクセス先特定情報を得るための演算アルゴリズムと演算パラメータを利用することによりこの条件は満たされる。そして、プロキシ装置はアクセス先特定情報を用いてネットワーク上のリモートホストと通信を行う。これにより、ＩＣカード装置はカード端末装置にアクセス先を知られることなく、リモートホストと通信を行うことが可能となる。

【００２１】第３に、ＩＣカード装置とプロキシ装置の二者間で暗号化に関するアルゴリズムと鍵情報を予め取り決め、この取り決めに基づいてカード端末装置に内容を知られることなく任意の情報をやりとりするための、セキュアパスを設ける。セキュアパスはＩＣカード装置とプロキシ装置間の両者が、この二者以外に情報を漏洩させることなく通信を行う、秘匿性を有する仮想的な通信経路である。これにより、ＩＣカード装置とプロキシ装置は、中間に位置するカード端末装置に内容を知られることなく、任意の情報を片方向もしくは双方向にて送受可能となる。上記第２に示したアクセス先情報の引き渡しは、このセキュアパスを用いて行うことができる。その場合、ＩＣカード装置内にてアクセス先情報を暗号化し（もしくは予め暗号化されたアクセス先情報を保持し）、この暗号化アクセス先情報をカード端末装置に引き渡し、カード端末装置はこれをそのままプロキシ装置に引き渡し、プロキシ装置は暗号化アクセス先情報を復号化して元のアクセス先情報を得る、という手順を踏むことにより行う。

【００２２】暗号化及び復号化の方法は、ＩＣカード装置とプロキシ装置の両者が予め保持する共通の鍵によって暗号化も復号化も行う対称鍵暗号方式、もしくはＩＣ

カード装置が公開鍵で暗号化を行い、プロキシ装置が対となる秘密鍵で復号化を行う非対称鍵暗号方式などの従来技術を適用すれば良い。また、カード端末装置から引き渡された暗号化アクセス先情報がカード端末装置によって捏造されたものではないことをプロキシ装置が確認するために、同じく非対称鍵暗号方式を応用した従来技術である署名を暗号化アクセス先情報に付与することもできる。また、アクセス先情報に限らず、セキュアパスを用いてＩＣカード装置とプロキシ装置の二者間で任意のデータを秘匿的にやりとりすることが可能である。

【００２３】第４に、上記セキュアパスを介してＩＣカード装置内におけるデータの暗号化手段を、アクセス先情報と、転送データ情報について個別に設ける。転送データ情報はプロキシ装置がさらにアクセス先のリモートホストに引き渡すデータ情報である。このとき、転送データの復号化については予めＩＣカード装置とリモートホストの二者間で取り決めておき、カード端末装置はもちろんプロキシ装置も転送データ復号用の鍵を持たないようにする。これにより、ＩＣカード装置がリモートホストに引き渡す転送データの内容を、カード端末装置だけでなくプロキシ装置にも隠蔽することが可能となる。同様に、リモートホストからＩＣカード装置に引き渡す転送データについても、ＩＣカードとリモートホストの二者間で取り決めた暗号化・復号化手段を用いることで、カード端末装置及びプロキシ装置に対して秘匿性を有する通信が可能となる。

【００２４】第５に、ＩＣカード装置にはＵＩリクエスト情報送信手段を設け、プロキシ装置にＵＩリクエスト情報受信手段を設ける。ＵＩリクエスト情報はＩＣカード装置がどのようなユーザインタフェース（ＵＩ）をカード端末装置上に実現するかを示す情報であり、これはセキュアパスを介してＩＣカード装置からプロキシ装置に引き渡される。もしくは、ＵＩリクエスト情報そのものにセキュリティを求める必要がない場合は、暗号化しない生データの状態でＵＩリクエスト情報を送受しても良い。また、プロキシ装置にＵＩ情報送信手段を設け、カード端末装置にＵＩ情報受信手段とＵＩ実行手段を設ける。プロキシ装置はＩＣカードから受け取ったＵＩリクエスト情報に基づき、カード端末装置がＵＩを実現するのに必要な情報をＵＩ情報送信手段から発し、カード端末装置はＵＩ情報受信手段にてそれを受け取る。ＵＩ情報としては、ユーザに対する画面表示に用いる文字フォント、文字フォントからレンダリングした文字列画像データ等を用いる。これにより、ＩＣカード装置が想定するＵＩ実現に必要な文字フォントがカード端末装置上に存在しない場合でも、ＩＣカード装置の想定通りの文字列情報をカード端末装置の表示画面上もしくは印刷結果としてユーザに提示することが可能となる。

【００２５】第６に、上記第５に示すＵＩ情報として、カード端末装置上に予め設けられた動作環境に適合するプログラム（実行手順と必要なデータを組にしたデータ列）を適用する。これにより、ＩＣカード装置が想定するＵＩが、カード端末装置に強く依存することなく独自のものとして実現可能となる。

【００２６】第７に、ＩＣカード装置とプロキシ装置のどちらか片方もしくは両方に、端末認証手段（利用機認証手段）と端末信頼度評価手段（利用機評価手段）を設ける。カード端末装置の認証は、予め定められた認証データもしくは定められた規則に基づく認証データ生成手段と、認証データをプロキシ装置もしくはＩＣカード装置に引き渡す認証データ送信手段をカード端末装置に設けることによって行う。プロキシ装置もしくはＩＣカード装置の端末認証手段は、カード端末装置の認証データ送信手段から受け取った認証データを読み取り、この認証データが予め定めた条件に合致するか否かを調べる。端末信頼度評価手段はこの認証結果を読み取り、条件に合致する場合はそのカード端末装置は信頼できる、合致しない場合は信頼できないとして信頼度の評価を行う。ここで、認証データの内容、生成方法、評価のための条件等は秘密のものとして扱い、信頼できないカード端末装置に漏洩しないようにする。また、認証データを複数種類とすることにより、評価結果をより細かく分類することも可能である。

【００２７】プロキシ装置がカード端末装置を認証、評価する場合は、ネットワーク上のアドレス情報等、偽証が困難なカード端末装置の固有情報を基にして行うことができる。その際、ネットワークアドレス情報と信頼度を対応付ける表を参照する等の方法を用いることにより、カード端末装置の信頼度に複数の段階を設けることもできる。これらにより、ＩＣカード装置もしくはプロキシ装置が、カード端末装置の信頼度を獲得することができる。

【００２８】第８に、ＩＣカード装置とプロキシ装置の両方に、端末信頼度評価手段を設けてカード端末装置の信頼度情報を共有する。この場合、片方の端末信頼度評価手段が得たカード端末装置の評価結果を、セキュアパスを通じて他方に渡すようにする。これにより、ＩＣカード装置もしくはプロキシ装置のいずれか片方がカード端末装置の信頼度を獲得できた場合、もう一方にその情報を渡すことが可能となる。また、両方が個別にカード端末装置の信頼度を獲得した場合は、それぞれの評価結果を互いに確認し合うことが可能となる。

【００２９】第９に、ＩＣカード装置に送信情報制御手段を設ける。送信情報制御手段は、上記第７もしくは第８でＩＣカード装置が得たカード端末装置の信頼度評価結果を読み取り、信頼度に応じてＩＣカード装置からカード端末装置に送信する情報の内容に対して変更、削除、追加等の処理を行う。これにより、ＩＣカード装置からカード端末装置に送信する情報内容をカード端末装置の信頼度に従って異なるものにすることができる。ま

た、ＩＣカード装置が機密情報として保持する情報をカード端末装置に送信しないよう上記送信情報制御手段を作用させる。機密情報の一つとして、ＩＣカード装置が保持するユーザの個人情報などがある。これにより、信頼度の低いカード端末装置には個人情報を送らないなど、カード端末装置毎に異なるセキュリティレベルを用いた情報管理が可能となる。

【００３０】第１０に、プロキシ装置に送信情報制御手段を設ける。これは上記第９に示したＩＣカード装置における送信情報制御手段と同様に、カード端末装置の信頼度評価結果に従ってプロキシ装置からカード端末装置に送信する情報の内容に対して変更、削除、追加等の処理を行う。また、ＩＣカード装置と同様に、プロキシ装置が保持する機密情報をカード端末装置に送信しないよう上記送信情報制御手段を作用させる。これらにより、プロキシ装置からカード端末装置に送信する情報内容を、上記のＩＣカード装置と同様にカード端末装置の信頼度に応じて異なるものにすることができ、信頼度の低いカード端末装置に機密情報を渡さないといったセキュリティ管理が可能となる。

【００３１】第１１に、プロキシ装置上において、上記第５に示したＵＩ情報送信手段に、上記第１０に示した送信情報制御手段を連動させ、カード端末装置の信頼度評価結果に従ってプロキシ装置からカード端末装置に送信するＵＩ情報に対して変更、削除、追加等の処理を行うようにする。カード端末装置の信頼度が低いと端末信頼度評価手段が判断した場合、送信情報制御手段が作用して、プロキシ装置からカード端末装置に送信するＵＩ情報のうち、ＩＣカード装置が持つ機密情報をカード端末装置上の表示画面装置に出力してしまうようなＵＩ部品を削除し、またＩＣカードのユーザがカード端末装置の入力装置を通じて機密情報を入力してしまうようなＵＩ部品を削除する。機密情報の一つとして、暗証番号、パスワード等がある。これらにより、信頼度の低いカード端末装置を使用する場合、機密情報をカード端末装置の画面上に表示し、それを取得されて漏洩してしまったり、また暗証番号等を不用意に入力して取得されてしまうようなトラブルの防止が可能となる。

【００３２】第１２に、ＩＣカード装置もしくはプロキシ装置に、機密情報変換手段を設ける。上記のカード端末装置によるＵＩ実行手段によって暗証番号、パスワード等の機密情報をユーザが直接入力する代わりに、機密情報を得るための第１の機密情報（仮の機密情報）を入力する。機密情報変換手段はこの第１の機密情報を読み取り、演算処理もしくは演算処理とデータ参照の組み合わせにより、第２の機密情報（真の機密情報）を生成する。機密情報変換手段をＩＣカード装置が備える場合は、生成した真の機密情報をセキュアパスを通じてプロキシ装置に渡す。その後、プロキシ装置は、真の機密情報を用いてリモートホストと通信を行う。これにより、カード端末装置のＵＩを通じて機密情報が漏洩する危険性を回避しつつ、機密情報を用いたネットワーク利用が可能となる。

【００３３】機密情報変換手段が機密情報生成のための演算を行う際のデータの一つとして、ランダムなデータ（無作為に選択されたデータ）を用い、ＵＩ実行手段がこのランダムデータをユーザに提示し、提示されたランダムデータに従って異なる仮の機密情報をユーザに入力するよう促すことで、真の機密情報の生成アルゴリズム等を推測されにくくなり、より安全性を増すことが可能となる。さらに、誤って真の機密情報を入力しないようユーザに促す表示をＵＩ実行手段が行うことで、ユーザの操作ミスによる機密情報漏洩を防止することが可能となる。

【００３４】第１３に、ＩＣカード装置にプロキシ選択手段を設ける。プロキシ選択手段は、予め定めたルールに従ってネットワーク上に存在する複数のプロキシ装置候補から、使用するプロキシ装置を決定する。ルールとしては、ＩＣカード装置が保持するプロキシ装置のリストから使用に適したプロキシ装置を逐次探す方法、ランダムで探す方法、またカード端末装置に問い合わせて最適候補を得る方法等がある。これらにより、ＩＣカード装置毎、カード端末装置毎などの条件に従って異なるプロキシ装置が利用可能となり、ネットワーク負荷及びプロキシの処理負荷の集中が緩和できる。また、プロキシ情報操作手段をＩＣカード装置に設ける。プロキシ情報操作手段は、ＩＣカード装置のユーザがカード端末装置等を通じて個々のプロキシ装置へのアクセス方法と使用ルールなどのプロキシ情報を登録・変更・削除するものである。これによりＩＣカード装置のユーザが使用するプロキシ装置を複数登録・変更することが可能となる。

【００３５】第１４に、ＩＣカード装置にインセンティブ発行手段を設け、カード端末装置にインセンティブ獲得手段を設ける。インセンティブ発行手段はインセンティブ獲得手段との間で電子情報の授受を行うことにより、カード端末装置及びカード端末装置の所有者や運用者に対して金銭的、事業的なメリットを直接的もしくは間接的に与える。インセンティブの例として広告情報を考えた場合、カード端末装置はＩＣカードユーザに対して商業広告等の情報を渡すことが可能となり、それが利用機運営のインセンティブとなる。また、インセンティブとして金銭もしくは何らかの有価物に関連した有価値情報を授受することにより、カード端末装置は、ＩＣカード装置から利用機使用の報酬としてより明確なインセンティブを得ることが可能となる。

【００３６】上記第１から第１４に関して、ＩＣカード装置としては、ＩＣカードに内蔵されるＩＣチップと同等もしくは類似した機能構成をもつ他の装置においても適用できる。装置の例として、ＩＣタグ、携帯電話機、携帯型情報端末、マイコン内蔵メモリカードなどが挙げ

られる。

【００３７】また、上記第１から第１４に関して、カード端末装置としては、不特定多数の人間が訪れる場所に設置する公共端末、不特定多数の人間が訪れる場所でレンタル品として貸し出される携帯電話機もしくは携帯型情報端末、不特定多数の人間にレンタル品として貸し出されるカーナビゲーション装置などを用いることができる。

【００３８】また、上記第１から第１４を構成する各装置を実現するためにコンピュータ上で動作するソフトウェアとして、磁気ディスク、光ディスク、半導体メディア等の情報記憶媒体に処理手順及びデータ等を格納しておき、コンピュータハードウェアがこれを読み取って所定の動作を行うようにしても、上記と同じ効果が得られる。

【００３９】したがって、本発明にかかるＩＣカードシステムにおいては、以下のような特徴的な構成を有する。

【００４０】（１）半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段とを備え、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストとデータ通信を行う際に、このリモートホストと前記カード端末装置との間に設けられるプロキシ装置と当該ＩＣカード装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するためのデータを前記プロキシ装置へ送信するもの。

【００４１】（２）前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を、前記カード端末装置が解釈困難なキーデータとして生成する通信キーデータ生成手段を備え、前記変換アルゴリズムもしくは変換パラメータとして、当該ＩＣカード装置と前記プロキシ装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いてデータ変換処理を実行する際に、前記通信キーデータを前記プロキシ装置へ送信するもの。

【００４２】（３）通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記プロキシ装置または前記リモートホストとの間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成するもの。

（４）前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記プロキシ装置との間で形成したセキュアパスを経由して該プロキシ装置へ送るもの。

【００４３】（５）前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第２の暗号処理手段を備え、前記第２の暗号処理手段により当該ＩＣカード装置が保持する任意のデータを暗号化し、この第２の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第２の暗号化データを前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送るもの。

【００４４】（６）前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第２の暗号処理手段を備え、前記第２の暗号処理手段により当該ＩＣカード装置が保持する任意のデータを暗号化し、この第２の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第２の暗号化データを前記リモートホストのアクセス先情報の暗号化データと共に前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送るもの。

【００４５】（７）当該ＩＣカード装置と前記プロキシ装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成するもの。

（８）当該ＩＣカード装置と前記プロキシ装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成するもの。

【００４６】（９）半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を、このカード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置に送信するＵＩリクエスト情報送信手段とを備えたもの。

【００４７】（１０）前記ＵＩリクエスト情報として、文字コードに関わる文字列情報を用いるもの。

（１１）前記ＵＩリクエスト情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させるためのプログラム情報による動作結果に影響を与えるパラメータ情報を用いるもの。

【００４８】（１２）半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置の認証を行

う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記プロキシ装置へ送るもの。

【００４９】（１３）半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記プロキシ装置から前記カード端末装置の信頼度評価結果を受け取るもの。

【００５０】（１４）前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えるもの。

（１５）前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してＩＣカード装置から送信する情報の一部もしくは全てを削除もしくは変更するもの。

【００５１】（１６）前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持する機密情報に関わる情報を削除もしくは変更するもの。

（１７）前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持するＩＣカードユーザのプライバシに関わる情報を削除もしくは変更するもの。

【００５２】（１８）半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段とを備え、前記機密情報変換手段は前記カード端末装置より入力された第１の機密情報データを当該カード端末装置に対して秘匿性を持った第２の機密情報データに変換し、この第２の機密情報データを前記カード端末装置と前記リモートホストとの間に設けられるプロキシ装置へ送るもの。

【００５３】（１９）前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてＩＣカードユーザに提示し、前記カード端末装置より入力された第１の機密情報データから前記変換キーデータを用いて前記第２の機密情報データを生成するもの。

（２０）前記変換キーデータと前記第１の機密情報データとを一対一に対応させて同一の第２の機密情報データを生成するための異なるデータの組を複数設けたもの。

【００５４】（２１）前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を前記プロキシ装置に送信するＵＩリクエスト情報送信手段を備え、前記ＵＩリクエスト情報として、前記リモートホストから要求される機密情報として前記第２の機密情報データの代わりに前記第１の機密情報データを入力すべきことをＩＣカードユーザに指示するためのＵＩ部品情報を用いるもの。

【００５５】（２２）予め定めた規則に従って計算機ネットワーク上の複数のプロキシ装置の中から一つを選択するプロキシ選択手段を備えたもの。

（２３）前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置を逐次的に検索して選択するもの。

（２４）前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置をランダムに検索して選択するもの。

（２５）前記プロキシ選択手段は、前記カード端末装置に問い合わせて使用に適するプロキシ装置を選択するもの。

（２６）使用に適するプロキシ装置を選択するためのプロキシ装置のリストを有し、このリスト内容の追加、変更、削除の少なくともいずれか一つを行うプロキシ情報操作手段を備えたもの。

【００５６】（２７）前記カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを発行するインセンティブ発行手段を備え、このインセンティブに関する情報を前記カード端末装置との間で通信するもの。

（２８）前記インセンティブとして広告情報を用い、前記インセンティブ発行手段は前記カード端末装置からこの広告情報を受信するもの。

（２９）前記インセンティブとして金銭あるいは有価値物に関連した有価値電子情報を用い、前記インセンティブ発行手段はこの有価値電子情報を前記カード端末装置

に送信するもの。

【００５７】（３０）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、前記ＩＣカード装置と当該プロキシ装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するデータ変換手段を備えたもの。

【００５８】（３１）前記データ変換手段は、前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を前記カード端末装置が解釈困難なキーデータとして生成した通信キーデータを変換するもので、前記変換アルゴリズムもしくは変換パラメータとして、当該プロキシ装置と前記ＩＣカード装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いて変換処理を行うもの。

【００５９】（３２）通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成するもの。

（３３）前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記ＩＣカード装置との間で形成したセキュアパスを経由して該ＩＣカード装置から受け取るもの。

【００６０】（３４）当該プロキシ装置と前記ＩＣカード装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成するもの。

（３５）当該プロキシ装置と前記ＩＣカード装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成するもの。

【００６１】（３６）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を受信するＵＩリクエスト情報受信手段と、前記受信したＵＩリクエスト情報の内容に基づいて前記カード端末装置におけるユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段とを備えたもの。

【００６２】（３７）前記ＵＩ情報として、文字フォントに関わる文字画像情報を用いるもの。

（３８）前記ＵＩ情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いるもの。

（３９）前記ＵＩ情報として、前記カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いるもの。

【００６３】（４０）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、前記カード端末装置の認証を行う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記ＩＣカード装置へ送るもの。

【００６４】（４１）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記ＩＣカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記ＩＣカード装置から前記カード端末装置の信頼度評価結果を受け取るもの。

（４２）前記端末認証手段と前記端末信頼度評価手段の少なくとも一方が、前記カード端末装置の計算機ネットワークへの接続に関わる固有かつ一意の情報を用いて動作するもの。

【００６５】（４３）前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えるもの。

（４４）前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置から送信する情報の一部もしくは全てを削除もしくは変更するもの。

（４５）前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する機密情報に関わる情報を削除もしくは変更するもの。

（４６）前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持するＩＣカードユーザまたはプロキシユーザのプライバシに関わる情報を削除もしくは変更するもの。

【００６６】（４７）前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記

カード端末装置に送信するＵＩ情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置からＵＩ情報を送信する前に、前記ＵＩ情報の中から機密情報表示に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のＵＩ情報を前記カード端末装置へ送るもの。

【００６７】（４８）前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があると認識された場合に、当該カード端末装置に対してプロキシ装置からＵＩ情報を送信する前に、前記ＵＩ情報の中から機密情報入力に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のＵＩ情報を前記カード端末装置へ送るもの。

【００６８】（４９）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段を備え、前記機密情報変換手段は前記カード端末装置より入力された第１の機密情報データを当該カード端末装置に対して秘匿性を持った第２の機密情報データに変換し、この第２の機密情報データを前記リモートホストへ送るもの。

【００６９】（５０）ＩＣカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたリモートホストとの間に設けられるＩＣカードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報に関して、前記カード端末装置より入力された第１の機密情報データが当該カード端末装置に対して秘匿性を持った状態に変換された第２の機密情報データを、前記ＩＣカード装置から受け取って前記リモートホストへ送る機密情報獲得手段を備えたもの。

【００７０】（５１）前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてＩＣカードユーザに提示し、前記カード端末装置より入力された第１の機密情報データから前記変換キーデータを用いて前記第２の機密情報データを生成するもの。

（５２）前記変換キーデータと前記第１の機密情報データとを一対一に対応させて同一の第２の機密情報データを生成するための異なるデータの組を複数設けたもの。

【００７１】（５３）前記カード端末装置において実現するユーザインタフェース部品に関わるＵＩ情報を前記カード端末装置に送信するＵＩ情報送信手段を備え、前記ＵＩ情報として、前記リモートホストから要求される機密情報として前記第２の機密情報データの代わりに前記第１の機密情報データを入力すべきことをＩＣカードユーザに指示するためのＵＩ部品情報を用いるもの。

【００７２】（５４）ＩＣカード装置とデータのやり取りを行うＩＣカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上において設けられるプロキシ装置と接続され、前記プロキシ装置から送られた当該カード端末装置におけるユーザインタフェース部品に関わるＵＩ情報を受信するＵＩ情報受信手段と、前記受信したＵＩ情報の内容に基づいて前記ＩＣカード装置とのデータ通信に関するユーザインタフェースを実行するＵＩ実行手段とを備えたもの。

【００７３】（５５）前記ＵＩ情報として、文字フォントに関わる文字画像情報を用いるもの。

（５６）前記ＵＩ情報として、当該カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いるもの。

（５７）前記ＵＩ情報として、当該カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いるもの。

【００７４】（５８）ＩＣカード装置とデータのやり取りを行うＩＣカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上において設けられる複数のプロキシ装置と接続され、前記ＩＣカード装置からの問い合わせに応じて、予め定めた規則に従って使用に適するプロキシ装置を選択するための処理を行うプロキシ選択処理手段を備えたもの。

【００７５】（５９）当該カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを受けるインセンティブ獲得手段を備え、このインセンティブに関する情報を前記ＩＣカード装置との間で通信するもの。

（６０）前記インセンティブとして広告情報を用い、前記インセンティブ獲得手段はこの広告情報を前記ＩＣカード装置に送信するもの。

（６１）前記インセンティブとして金銭あるいは有価値物に関連した有価値電子情報を用い、前記インセンティブ獲得手段は前記ＩＣカード装置からこの有価値電子情報を受信するもの。

【００７６】（６２）上記（１）～（２９）のいずれかに記載のＩＣカードシステム用のＩＣカード装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

（６３）上記（３０）～（５３）のいずれかに記載のＩＣカードシステム用のプロキシ装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情

報記録媒体。

（６４）上記（５４）～（６１）のいずれかに記載のＩＣカードシステム用のカード端末装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【００７７】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

【００７８】［第１実施形態］図１は本発明の第１実施形態に係るＩＣカードシステムの構成を示すブロック図である。

【００７９】本実施形態のＩＣカードシステムは、半導体記憶手段を搭載したカード本体を含むＩＣカード装置に相当するＩＣカード１０１、ＩＣカード１０１とデータ通信を行うカード端末装置に相当する利用機１０２、ＩＣカード１０１に対して情報の提供等を行うホストコンピュータであるリモートホスト１０４、利用機１０２とリモートホスト１０４との間に設けられＩＣカード１０１とリモートホスト１０４の両者に対してデータ通信を行うプロキシ装置１０３を備えて構成される。利用機１０２とプロキシ装置１０３の間、及びプロキシ装置１０３とリモートホスト１０４の間は、インターネット等の計算機ネットワーク１０５によって接続されている。なお、利用機１０２とリモートホスト１０４は、共通の計算機ネットワークに接続されていても、また異なる計算機ネットワークに接続されていても良いが、プロキシ装置１０３は、利用機１０２及びリモートホスト１０４の両者とそれぞれ共通の計算機ネットワークに接続され、両者と通信が可能なように構成されている。

【００８０】利用機１０２にはＩＣカードリーダライタ１０８が設けられている。ＩＣカード１０１として接触型ＩＣカードを適用した場合、ＩＣカード１０１はＩＣカードリーダライタ１０８に挿入もしくは接続され、電気信号を用いて利用機１０２と通信を行う。また、ＩＣカード１０１に非接触型ＩＣカードを適用した場合には、ＩＣカード１０１はＩＣカードリーダライタ１０８との間で電波信号をやりとりすることにより、利用機１０２と通信を行う。

【００８１】ＩＣカード１０１は、内部に送信用データ保持手段１０６とデータ送信手段１０７とを備えている。送信用データ保持手段１０６は、ＩＣカード１０１に内蔵されるＩＣチップのメモリ等を用いて実現される。データ送信手段１０７は、送信用データ保持手段１０６が保持するデータを読み取ってＩＣカードリーダライタ１０８に送信するもので、ＩＣカード１０１に内蔵される通信ハードウェア及びそれを駆動するための処理装置とソフトウェアプログラムによって実現される。

【００８２】なお、以下の実施形態において示す機能的構成による各手段は、前記データ送信手段１０７と同様に、各構成装置がもつハードウェアと、それを駆動するための処理装置及びソフトウェアプログラムにより実現されるものである。

【００８３】利用機１０２は、内部にＩＣカードリーダライタ１０８からデータを受け取るデータ受信手段１０９と、データ受信手段１０９が受信したデータを計算機ネットワーク１０５を介してプロキシ装置１０３に送信するデータ転送手段１１０とを備えている。

【００８４】プロキシ装置１０３は、内部に計算機ネットワーク１０５を介して利用機１０２から受信したデータを別のデータに変換するデータ変換手段１１１を備えている。このプロキシ装置１０３は、データ変換手段１１１が作成した変換後のデータを、計算機ネットワーク１０５を介してリモートホスト１０４に送信し、リモートホスト１０４はこれを受信する。

【００８５】ＩＣカード１０１が利用機１０２を介してプロキシ装置１０３と通信を開始するに先立って、予めＩＣカード１０１内のアプリケーションプログラムとプロキシ装置１０３のデータ変換手段１１１との間で、データ変換の規則と方法についての取り決めを作っておく。

【００８６】例えば、ｘというデータを与えた場合はｆ（ｘ）というデータに変換される規則とし、変換方法ｆについてＩＣカード１０１とプロキシ装置１０３のみが知っている状態を作る。この取り決めはＩＣカード１０１の発行以前に行っても良いし、ＩＣカード１０１の発行後も、ＩＣカード１０１とプロキシ装置１０３との間で充分にセキュアな通信が可能な条件下であれば行うことができる。

【００８７】ＩＣカード１０１のユーザがリモートホスト１０４にデータを送信する場合、ＩＣカード１０１の送信用データ保持手段１０６にデータｘを格納し、データ送信手段１０７はこのデータｘを利用機１０２のＩＣカードリーダライタ１０８を介してデータ受信手段１０９に送る。次に、データ受信手段１０９はデータ転送手段１１０にデータｘを渡し、データ転送手段１１０はデータｘを計算機ネットワーク１０５を介してプロキシ装置１０３のデータ変換手段１１１に送る。

【００８８】ここで、利用機１０２は変換方法ｆを知らないため、プロキシ装置１０３の内部でデータ変換手段１１１が出力するデータｆ（ｘ）を知ることはできない。よって、プロキシ装置１０３がｆ（ｘ）を用いてリモートホスト１０４と通信を行えば、結果としてＩＣカード１０１のユーザは利用機１０２に知られることなくデータｆ（ｘ）を用いた通信をリモートホスト１０４との間で行うことが可能となる。

【００８９】特に、ｆ（ｘ）を逆変換可能なものに定め、ｆの逆変換をｇ（ｙ）としたとき、ＩＣカード１０１はｇ（ｙ）を送信用データ保持手段１０６に置くことにより、データｙを利用機１０２に知られることなくリモートホスト１０４に送ることが可能となる。その際、

リモートホスト１０４にはｆ（ｘ）を得るためのデータ変換手段は不要である。さらに、プロキシ装置１０３はそれ自身がネットワークを利用してリモートホスト１０４と通信を行えるため、従来は利用機１０２に依存していたネットワーク通信、ユーザインタフェース形成等に関わる情報を全て利用機１０２に秘匿しつつ、プロキシ装置１０３が得ることが可能となる。

【００９０】上記のようなプロキシ装置は不正侵入が困難な安全な建物内等に設置することが容易であり、これは街頭等の不特定多数の人間が出入りする場所に置かれる利用機と比較してセキュリティ強度を容易に高めることが可能である。通常、キオスク端末用として専用に作られた計算機は特に強固なセキュリティを確保したハードウェアを使用するが、本実施形態によれば、そのようなハードウェアを使用しなくともＩＣカードユーザに被害を及ぼし難い利用機を設置できる。また、ＩＣカードユーザもセキュリティ強度の弱い利用機を安全に利用できることになり、その実用的効果は大きい。

【００９１】このように、本実施形態の構成では、ＩＣカードユーザは利用機に通信内容を知られることなくＩＣカードとプロキシ装置との間で通信を行うことができるため、アクセス先や通信内容を秘匿してセキュリティを確保した状態で利用機を使用することが可能となる。よって、利用機において必ずしも強固なセキュリティ上の保証をする必要がなく、利用機設置に関するハードウェア価格や運営コストを低減することも可能である。ＩＣカードユーザは、街頭等の不特定多数の人間が訪れる場所に設置ている場合など、利用機の信頼度が不明確な場合であっても十分なセキュリティを確保でき、安心して使用することができる。

【００９２】［第２実施形態］図２は本発明の第２実施形態に係るＩＣカードシステムの構成を示すブロック図である。第２実施形態は、第１実施形態と同様に、インターネット上のサービスを受けるアプリケーションを搭載したＩＣカード２０１、リモートホスト２０４を備えて構成される。これらは、図２で模式的に示すインターネット空間２０５に設けられる。利用機２０２とプロキシ装置２０３、及びプロキシ装置２０３とリモートホスト２０４は、それぞれインターネット空間２０５において形成されるネットワークコネクション（仮想的なデータ通信経路を持つ関係）２０６、２０７により接続される。なお、個々の装置が具備する手段は図１の第１実施形態と同様である。

【００９３】ＩＣカード２０１に載せるアプリケーションとしては、インターネット上のリモートホスト２０４（World Wide Webサービスを提供するウェブサイト）へアクセスし、リモートホスト２０４からの情報をＩＣカード２０１内のメモリに取得、もしくはＩＣカード２０１内のメモリに保持している情報をリモートホスト２０４に登録するソフトウェアを想定する。

【００９４】図３は、本実施形態におけるアクセス先情報及び通信キーデータの関係を例示したものである。ここで、符号３０１はＩＣカード２０１のアプリケーションがアクセスしようとするリモートホスト２０４のインターネットにおける存在場所（ＵＲＬ）を記したアクセス先情報であり、符号３０２はアクセス先情報３０１から第１実施形態に示した変換ｇによって得た通信キーデータである。なお、アクセス先情報３０１と変換ｇは省略し、初めから変換済みの通信キーデータ３０２を保持していても良い。また、符号３０３及び３０４は通信キーデータ３０２がそれぞれ利用機２０２とプロキシ装置２０３に渡った状態を示すもので、通信キーデータ３０２と同一のものである。符号３０５は通信キーデータ３０４から変換ｆによって得られるアクセス先情報であり、アクセス先情報３０１と同一のものとなる。

【００９５】図４は本実施形態におけるアクセス先秘匿処理の流れを示したフローチャートであり、図１～３と合わせて以下その動作を説明する。ＩＣカード２０１のユーザは、ＩＣカード２０１を利用機２０２に挿入することにより上記のインターネットサービスを受けられる。ここで利用機２０２は、例えば街頭、駅、公共施設、店舗等に置かれた共用端末で、不特定多数のユーザが利用することを前提に設置され、ＩＣカード２０１のユーザは利用機２０２の運用、管理のポリシー等について知らされていない状況を想定する。

【００９６】ＩＣカード２０１は、まずアクセス先のＵＲＬ（Uniform Resource Locator；サービス提供ホストのインターネット空間におけるホスト特定情報（ドメイン名及びサーバ名など）と基本的な通信プロトコルとを含んだ文字情報）を示すアクセス先情報３０１をｇで変換し（ステップ４０１）、通信キーデータ３０２を生成して送信用データ保持手段１０６に格納する（ステップ４０２）。次いで、データ送信手段１０７を用いて通信キーデータ３０２をＩＣカードリーダライタ１０８を介して利用機２０２に送信する（ステップ４０３）。

【００９７】次に、利用機２０２はデータ受信手段１０９を用いて通信キーデータ３０３を受信する。（ステップ４０４）。続いて、利用機２０２はプロキシ装置２０３と通信するためのネットワークコネクション２０６をインターネット空間２０５内に形成する（ステップ４０５）。なお、コネクション形成の際に用いるプロキシ装置２０２のＵＲＬは、利用機２０２が予め保持しておいても良いし、既知のＩＣカード・利用機間通信技術を用いてＩＣカード２０１から利用機２０２に伝達しても良い。

【００９８】ネットワークコネクション２０６を形成した後、利用機２０２はデータ転送手段１１０を用いて通信キーデータ３０３を内容を改変せずにプロキシ装置２０３に送信し（ステップ４０６）、プロキシ装置２０３はこれを通信キーデータ３０４として受信する（ステッ

プ４０７）。利用機２０２が通信キーデータ３０３を改変せずに転送したことは、既知のデータ照合技術を用いて確認できる。

【００９９】次に、プロキシ装置２０３はデータ変換手段１１１を用いて通信キーデータ３０４に対し変換ｆを行い（ステップ４０８）、ＩＣカード２０１が意図した通りのアクセス先情報３０５を獲得する（ステップ４０９）。最後に、プロキシ装置２０３は獲得したアクセス先情報３０５から得たリモートホスト２０４の情報（ＵＲＬ等）を用いて、インターネット空間２０５内にネットワークコネクション２０７を形成する（ステップ４１０）。

【０１００】なお、本実施形態ではアクセス先情報３０１及び３０５をＵＲＬとした構成例を示したが、その他のホスト特定情報及び通信方法特定情報によって構成することもできる。また、本実施形態では計算機ネットワークとしてインターネットを適用した構成例を示したが、無線ネットワークを含めたその他の計算機ネットワークによって構成することもできる。

【０１０１】また、本実施形態に示した処理フローに先立ち、従来の認証技術を用いてＩＣカード２０１とプロキシ装置２０３の両者間で認証を行うことにより、利用機２０２とプロキシ装置２０３が示し合わせてＩＣカード２０１を騙すことによる不正行為を防止することができる。この不正行為の例としては、プロキシ装置２０３が獲得したアクセス先情報３０５を、プロキシ装置２０３自身が利用機２０２に教えてしまうことが考えられる。なお、このような不正行為を防止するために、ＩＣカード２０１はプロキシ装置２０３に情報を渡す処理に先立ち、プロキシ装置２０３が正当でかつ安全であることを確認すべきである。これは本発明における他の実施形態においても同様である。

【０１０２】以上のように、ＩＣカードが発する通信キーデータを図３のようにプロキシ装置がアクセス先情報に変換することによって、利用機がリモートホストに対して直接ネットワークコネクションを形成することなくなるため、ＩＣカード上のアプリケーションが計算機ネットワーク上のどのホストに、どのような方法でアクセスしたかの情報が利用機を通じて漏洩する問題が回避され、その実用的効果は大きい。この本実施形態の手段によって、［発明が解決しようとする課題］の欄に示した第１の問題点を明確に解決することができる。

【０１０３】［第３実施形態］図５は本発明の第３実施形態に係るＩＣカードシステムの構成を示すブロック図である。第３実施形態は、第１実施形態と同様に、ＩＣカード５０１、利用機５０２、プロキシ装置５０３、リモートホスト５０４を有して構成され、利用機５０２とプロキシ装置５０３、及びプロキシ装置５０３とリモートホスト５０４はそれぞれ計算機ネットワーク５０５を介して接続される。利用機５０２はＩＣカードリーダライタ５０６を具備している。これらは図１の第１実施形態における各装置と同様な構成要素を持っている。

【０１０４】ＩＣカード５０１は、内部に既知の暗号技術を用いて情報の暗号化及び復号化を行う暗号処理手段５０７を備えている。プロキシ装置５０３は、内部に暗号処理手段５０７と対になって一方が暗号化した情報を他方が復号化する暗号処理手段の機能を併せ持ったデータ変換手段５０８を備えている。これらの暗号処理手段５０７とデータ変換手段（暗号処理手段）５０８との間には、セキュアパス５０９が形成される。

【０１０５】このセキュアパス５０９は、ＩＣカード５０１の暗号処理手段５０７が暗号化したデータを第１実施形態と同様の方法でプロキシ装置５０３のデータ変換手段５０８に渡すことによって、利用機５０２に内容を秘匿しながら情報を伝達することにより形成されるセキュアな（所望のセキュリティを確保した）仮想的データ通信経路である。また、プロキシ装置５０３のデータ変換手段５０８が情報の暗号化を行い、第１実施形態と逆方向にデータを送信し、さらにＩＣカード５０１の暗号処理手段５０７が情報を復号化することにより、セキュアパス５０９は双方向のデータ通信経路となる。プロキシ装置５０３は、セキュアパス５０９を通じてＩＣカード５０１から得た情報を用いてリモートホスト５０４と通信を行い、またリモートホスト５０４から得た情報をセキュアパス５０９を通じてＩＣカード５０１に渡す。

【０１０６】以上のように、本実施形態ではＩＣカード５０１とプロキシ装置５０２の間にセキュアパス５０９を設けることにより、利用機５０２に内容を秘匿しながらＩＣカード５０１とリモートホスト５０４との間の通信が可能となる。その際、リモートホスト５０４にはＩＣカード５０１の暗号処理手段５０７と対になる暗号処理手段を付加する必要がない。このため、リモートホスト５０４として既存のインターネットサービスホストを適用した場合、ホストの構成を変更せずにＩＣカード５０１との間でセキュアなデータ送受が可能となる。

【０１０７】また、サービスの性格によってプロキシ装置５０３とリモートホスト５０４の間で独自のセキュリティ処理を施すことも容易であり、あるいはプロキシ装置５０３とリモートホスト５０４の間ではセキュリティ手段を設けず、課金等に関するセキュアな処理は全てプロキシ装置５０３が行うというような適用も可能であり、その実用的効果は大きい。

【０１０８】［第４実施形態］第４実施形態として、図２に示したＩＣカードシステムの構成、図３に示したデータフロー及び図４に示した処理フローと同様の処理を、図５に示したセキュアパスを用いて実現したシステムも例示できる。すなわち、ＩＣカード２０１が保持するアクセス先情報３０１を、暗号処理手段５０７を用いて暗号化し、セキュアパス５０９を通じてプロキシ装置２０３のデータ変換手段５０８に渡し、アクセス先情報

３０５を得るものである。

【０１０９】この実施形態では、第２実施形態と同等の効果が得られるが、さらにセキュアパスを使うことにより、アクセス先のみでなくネットワークコネクション形成後の通信内容も全て利用機に対して秘匿できる効果がある。第４実施形態によって、第２実施形態と同様に［発明が解決しようとする課題］の欄に示した第１の問題点を明確に解決することができる。

【０１１０】［第５実施形態］図６は本発明の第５実施形態に係るＩＣカードシステムの構成を示すブロック図である。第５実施形態は、第１実施形態と同様に、ＩＣカード６０１、利用機６０２、プロキシ装置６０３、リモートホスト６０４を有して構成され、利用機６０２とプロキシ装置６０３、及びプロキシ装置６０３とリモートホスト６０４はそれぞれ計算機ネットワーク６０５を介して接続される。利用機６０２はＩＣカードリーダライタ６０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０１１１】ＩＣカード６０１は、内部に既知の暗号技術を用いて情報の暗号化及び復号化を行う第１の暗号処理手段６０７及び第２の暗号化手段６１０を備えている。第１の暗号処理手段６０７と第２の暗号化手段６１０とは、互いに異なる暗号処理の仕組を用いるか、もしくは同一の暗号処理の仕組を異なる鍵を用いて利用する構成をとる。プロキシ装置６０３は、内部に第１の暗号化手段６０７と対になってセキュアパス６０９を形成する第１の復号化手段６０８を備えている。また、リモートホスト６０４は、内部に第２の暗号化手段６１０と対になってセキュアパス６１２を形成する第２の復号化手段６１１を備えている。

【０１１２】この場合、初めは第２の暗号化手段６１０が生成した暗号化データはセキュアパス６０９を介してプロキシ装置６０３に渡す。もしくは、利用機６０２による復号が困難であるという条件を満足すれば、セキュアパス６０９を介さずにプロキシ装置６０３に渡しても良い。いずれの場合もプロキシ装置６０３は第２の暗号化手段６１０が生成したデータをそのままリモートホスト６０４に転送する。これにより、ＩＣカード６０１とリモートホスト６０４を直接結ぶ新たなセキュアパス６１２が形成される。

【０１１３】なお、本実施形態では各暗号化手段と各復号化手段の働きで各セキュアパスを単一方向の通信に用いる例で説明したが、暗号化と復号化を逆に用いる構成を採ることにより、各セキュアパスを双方向通信に用いることも可能である。

【０１１４】上記のように、本実施形態によれば、ＩＣカード６０１のユーザ及びＩＣカード６０１内に設けたアプリケーションは、セキュアパス６０９を用いて利用機６０２に情報を秘匿しながらプロキシ装置６０３とセキュアな通信を行うことができ、さらにセキュアパス６１２を用いて利用機６０２に情報を秘匿しながらリモートホスト６１１とセキュアな通信を行うことができる。さらに、各暗号化手段及び復号化手段の暗号強度を充分に確保すれば、利用機及びプロキシ装置以外にも、データ通信経路上の様々な装置もしくは手段による情報の漏洩を防ぐことが可能となり、その実用的効果は大きい。

【０１１５】［第６実施形態］第６実施形態として、図６の構成において、ＩＣカード６０１からプロキシ装置６０３へ、セキュアパス６０９を用いてリモートホスト６０４のアクセス先情報を渡し、さらにＩＣカード６０１からリモートホスト６０４へ、セキュアパス６１２を用いてアクセス先情報以外の任意の情報を渡すようなシステムも例示できる。この場合、第５実施形態の効果に加えて、ＩＣカード６０１とリモートホスト６０４の間において、利用機６０２だけでなくプロキシ装置６０３に対しても情報を秘匿した通信を可能にする効果がある。

【０１１６】［第７実施形態］第７実施形態として、図５における暗号処理手段５０７、データ変換手段５０８、あるいは図６における第１の暗号化手段６０７、第１の復号化手段６０８、第２の暗号化手段６１０、第２の復号化手段６１１を、それぞれ相互に対応関係を持つ手段間において共通の鍵を用いる対称鍵暗号方式を用いて実現したシステムも例示できる。この実施形態によれば、第３～第６実施形態と同等の効果が得られる。

【０１１７】［第８実施形態］第８実施形態として、図５における暗号処理手段５０７、データ変換手段５０８、あるいは図６における第１の暗号化手段６０７、第１の復号化手段６０８、第２の暗号化手段６１０、第２の復号化手段６１１を、それぞれ相互に対応関係を持つ手段間において互いに対応付けられた異なる鍵を用いる非対称鍵暗号方式を用いて実現したシステムも例示できる。非対称暗号方式としては既知の公開鍵暗号方式が適用できる。

【０１１８】また、第７実施形態に示した構成と組み合わせて、非対称暗号によって対称鍵暗号を渡し、セキュアパスを流れる情報の一部を対称鍵暗号を用いて秘匿化することもできる。この場合、第３～第６実施形態と同等の効果が得られる他、鍵交換の簡便性と暗号処理の高速性を得ることができる効果がある。

【０１１９】［第９実施形態］図７は本発明の第９実施形態に係るＩＣカードシステムの構成を示すブロック図である。第９実施形態は、第１実施形態と同様に、ＩＣカード７０１、利用機７０２、プロキシ装置７０３、リモートホスト７０４を有して構成され、利用機７０２とプロキシ装置７０３、及びプロキシ装置７０３とリモートホスト７０４はそれぞれ計算機ネットワーク７０５を介して接続される。利用機７０２はＩＣカードリーダライタ７０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０１２０】ＩＣカード７０１は、ＩＣカード７０１のユーザもしくはアプリケーションが求めるユーザインタフェース（以下、適宜ＵＩと略記する）に関わる情報（以下、ＵＩリクエスト情報と記する）を送信するＵＩリクエスト情報送信手段７０７を備えている。プロキシ装置７０３は、前記ＵＩリクエスト情報を受けるＵＩリクエスト情報受信手段７０８と、利用機７０２におけるユーザインタフェースの形成と動作に関わる情報（以下、ＵＩ情報と記する）を送信するＵＩ情報送信手段７０９とを備えている。また、利用機７０２は、前記ＵＩ情報を受けるＵＩ情報受信手段７１０と、ユーザインタフェースの形成及び動作の処理を行うＵＩ実行手段７１１とを備えている。

【０１２１】ＩＣカード７０１は、ＵＩリクエスト情報送信手段７０７を用いてＵＩリクエスト情報をＩＣカードリーダライタ７０６を介して利用機７０２に渡し、さらに利用機７０２により計算機ネットワーク７０５を介してプロキシ装置７０３のＵＩリクエスト情報受信手段７０８に渡す。プロキシ装置７０３は、ＵＩ情報送信手段７０９を用いて、受信したＵＩリクエスト情報に基づいて生成したＵＩ情報を計算機ネットワーク７０５を介して利用機７０２のＵＩ情報受信手段７１０に渡す。

【０１２２】図８は本実施形態におけるＵＩ制御処理の流れを示したフローチャートであり、図７と合わせて以下その動作を説明する。ＩＣカード７０２に搭載したアプリケーションが利用機７０２を通じてユーザとインタラクション（入出力の受け答え）を取る場合、まずＩＣカード７０２はどのようなＵＩを必要とするのかを情報化したＵＩリクエスト情報を生成する（ステップ８０１）。次いで、ＵＩリクエスト情報送信手段７０７が前記のＵＩリクエスト情報を、利用機７０２を介してプロキシ装置７０３に送信する（ステップ８０２）。

【０１２３】そして、プロキシ装置７０３のＵＩリクエスト情報受信手段７０８がＵＩリクエスト情報を受け取り（ステップ８０３）、このＵＩリクエスト情報を用いて利用機におけるＵＩ形成と動作に関わるＵＩ情報を生成し（ステップ８０４）、ＵＩ情報送信手段７０９が利用機７０２に送信する（ステップ８０５）。

【０１２４】次に、利用機７０２のＵＩ情報受信手段７１０がプロキシ装置７０３からＵＩ情報を受信し（ステップ８０６）、このＵＩ情報を用いてＵＩ実行のための詳細な情報を生成する（ステップ８０７）。そして、利用機７０２が持つ画面装置、キー入力装置、ポインティング装置等のハードウェアを駆動してＵＩを実行する（ステップ８０８）。

【０１２５】その後、利用機７０２上のＵＩによる入出力を反映させながら、ＩＣカード７０１のアプリケーションはリモートホスト７０４からサービスを受ける。その際、リモートホスト７０４との通信はプロキシ装置７０３を介しても良いし、利用機７０２が直接行っても良い。また、ＩＣカード７０１のアプリケーションが使用するサービスがプロキシ装置７０３までで閉じている場合は、リモートホスト７０４は構成要素に含める必要はない。

【０１２６】このように、本実施形態では、ＩＣカード７０１が発するＵＩリクエスト情報から、プロキシ装置７０３内でＵＩ情報を生成して利用機７０２に送り、利用機７０２では受信したＵＩ情報からＵＩを形成し実行することにより、ＩＣカードユーザは適切なＵＩを利用機上で使用できる。その際、ＵＩリクエスト情報を送ることでＩＣカード７０１に収めることのできない大容量の情報をＵＩ情報に含むことが可能となり、その実用的効果は大きい。

【０１２７】［第１０実施形態］第１０実施形態として、前述した第９実施形態におけるＵＩ制御処理の具体例を示す。ＩＣカードシステムの構成と処理の流れは第９実施形態と同様である。図９はＩＣカードシステムにおけるＵＩリクエスト情報及びＵＩ情報のデータ構造、並びにＵＩ実行結果の一例を示す動作説明図である。

【０１２８】図９（Ａ）に示すように、ＩＣカード７０１のＵＩリクエスト情報送信手段７０７が発するＵＩリクエスト情報９０１は、表示位置情報９０２、文字属性情報９０３及び文字列情報９０４からなり、文字列情報９０４は文字列を構成する文字コードの配列を有し、最後の配列要素に終端記号を格納する。なお、文字列情報９０４は終端記号の代わりに文字列配列の先頭もしくはそれ以前に文字数を格納したデータ構造を採っても良い。

【０１２９】図９（Ｂ）に示すように、プロキシ装置７０３のＵＩ情報送信手段７０９が発するＵＩ情報９０５は、表示位置情報９０６及び画像イメージ情報９０７からなる。また、図９（Ｃ）はＵＩ情報９０５に基づいて利用機７０２において実行されるＵＩ実行結果９０８を示したものである。液晶表示パネル（ＬＣＤ）等からなる表示画面装置９０９内に表示されるウィンドウ領域９１０において、文字列画像９１１が表示されている。ここで、符号９１２及び９１３は文字列画像９１１の表示位置であり、それぞれウィンドウ領域９１０の左端及び上端からの距離を用いて表される。なお、表示位置の取り方は他にも様々な方法があり、どの方法を用いても良い。

【０１３０】次に、本実施形態における処理の流れを説明する。図８で示した処理のステップ８０１で、ＩＣカード７０１はＵＩリクエスト情報９０１を生成する。文字列情報９０４には、ＩＣカード７０１のアプリケーションが利用機７０２を通じてユーザに見せようとする文字列の個々の文字コードを格納する。また、表示位置情報９０２には文字列を表示させようとする位置を示したデータを格納し、文字属性情報９０３には文字のフォント、色、大きさ、装飾等、表示内容を決定する際に必要

な情報を格納する。

【０１３１】そして、ステップ８０３でＵＩリクエスト情報９０１を受け取ったプロキシ装置７０３は、続くステップ８０４で、文字属性情報９０３と文字列情報９０４及びプロキシ装置が持つ文字フォントデータを用いて文字列を視覚的に表現した画像イメージ情報９０７を生成する。さらに、表示位置情報９０２を加工もしくはそのままのデータ内容で表示位置情報９０６を生成し、これらの画像イメージ情報９０７と表示位置情報９０６とをまとめてＵＩ情報９０５を生成する。

【０１３２】次に、ステップ８０６でＵＩ情報９０５を受け取った利用機７０２は、続くステップ８０７で、表示位置情報９０６及び画像イメージ情報９０７を取り出し、必要であれば利用機７０２自身のハードウェア及びソフトウェアの条件に適合したデータ内容に変換する。その後、ステップ８０７で利用機７０２の表示画面装置９０９内のウィンドウ領域９１０に、表示位置９１２、９１３にて文字列画像９１１を表示する。

【０１３３】なお、本実施形態では、ＵＩ情報９０５に含まれる画像イメージ情報９０７を、文字列全体を表現した単一の画像データで構成する例を示したが、画像イメージ情報９０７を細分化して個々の文字に対応した画像データを複数格納する方法においても同様に実施可能である。また、ＵＩリクエスト情報９０１に含まれる文字列情報９０４には、終端記号だけでなく改行等の文字列制御情報を含むこともでき、その場合ＵＩ情報生成時もしくはＵＩ実行時に制御情報に対応した処理を行うことで各種文字列制御が実施可能である。

【０１３４】また、ＵＩ情報９０５の生成及び受け渡し以前に、プロキシ装置７０３が利用機７０２に対して、使用しようとするフォントデータを持っているかどうかを問い合わせ、持っていない場合は上記のように画像データとして送り、既に持っている場合は文字コードを送る、という方法も実施可能である。また、本実施形態では利用機７０２のＵＩ実行手段７１１として表示画面装置９０９を適用した例で説明したが、その他プリンタなどの印刷装置等についても同様に実施可能である。

【０１３５】このように、本実施形態では、ＵＩリクエスト情報９０１に文字コードを含め、ＵＩ情報９０５に文字コードに対応した画像イメージを含めることにより、利用機７０２が持っていない文字フォントによる文字情報であっても、ＩＣカード７０１からのリクエストにより使用可能となる。さらにＩＣカード７０１にフォントデータを置くことなく実現することができるので、ＩＣカード７０１において大量の文字情報を格納しておく必要がなく、データ記憶容量を削減でき、その実用的効果は大きい。

【０１３６】［第１１実施形態］第１１実施形態として、前述した第９実施形態におけるＵＩ制御処理の第１の変形例を示す。ＩＣカードシステムの構成と処理の流れは第９実施形態と同様である。第１１実施形態では、ＵＩ情報には、利用機７０２のハードウェアを利用してユーザインタフェースとして動作させるためのプログラム情報を適用し、ＵＩリクエスト情報には前記のプログラムが実行時に使用するパラメータ情報を適用する。ＵＩ情報にはプログラム情報の他に任意のデータ情報を含むこともでき、また、ＵＩリクエスト情報によって前記データ情報もしくはプログラム情報自体を動的に生成しても良い。

【０１３７】本実施形態の場合、図８のフローチャートにおいては、ステップ８０６で利用機７０２に渡されたＵＩ情報は、ステップ８０８でＵＩ実行手段７１１によってプログラムとして解釈され、実行される。

【０１３８】ここで、ＵＩリクエスト情報を、利用機７０１の表示画面装置上に表示する文字、ボタン、入力領域等のユーザインタフェース部品の情報から構成し、ＵＩ情報をこれらのユーザインタフェース部品を配置し駆動するプログラムとすることにより、ＩＣカード７０１のアプリケーションが意図する様々なユーザインタフェースを利用機７０２上で実行することができる。プログラムの構成は、利用機７０２のハードウェアに依存した機械語コードを用いるか、もしくは利用機７０２に特定の言語のインタプリタもしくはプログラムを実行する仮想マシンを搭載し、それらの上で動作するプログラムコードを適用する。

【０１３９】このように、第１１実施形態によれば、ＵＩ情報としてプログラム情報を適用することにより、利用機７０２上で柔軟なユーザインタフェースを実行することができ、その実用的効果は大きい。

【０１４０】［第１２実施形態］第１２実施形態として、前述した第９実施形態におけるＵＩ制御処理の第２の変形例を示す。ＩＣカードシステムの構成と処理の流れは第９実施形態と同様である。また、ＵＩ情報としてプログラム情報を適用する点において第１１実施形態と同様である。

【０１４１】第１２実施形態では、図８のフローチャートにおけるステップ８０４でＵＩ情報を生成する前に、プロキシ装置７０３が保持する利用機７０２に関する情報を用いるか、もしくはプロキシ装置７０３が利用機７０２に問い合わせを行うことによって利用機７０２の構成等の情報を獲得し、それに基づいてＵＩ情報に含まれるプログラムの内容を異なるものにする。

【０１４２】例えば、利用機７０２が持つ表示画面装置の大きさや解像度に応じて、ユーザインタフェース部品の配置や大きさを変更したり、入力装置の種類によって異なるユーザインタフェース部品を配置したりすることができる。

【０１４３】このように、第１２実施形態によれば、ＵＩ情報として用いるプログラム情報を利用機７０２の条件に基づいて異なるものにすることにより、利用機７０

２が様々な種類の構成要素からの選択により構成される場合でも適切なユーザインタフェースを得ることが可能となり、その実用的効果は大きい。

【０１４４】［第１３実施形態］図１０は本発明の第１３実施形態に係るＩＣカードシステムの構成を示すブロック図である。第１３実施形態は、第１実施形態と同様に、ＩＣカード１００１、利用機１００２、プロキシ装置１００３、リモートホスト１００４を有して構成され、利用機１００２とプロキシ装置１００３、及びプロキシ装置１００３とリモートホスト１００４はそれぞれ計算機ネットワーク１００５を介して接続される。利用機１００２はＩＣカードリーダライタ１００６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０１４５】ＩＣカード１００１は、利用機１００２と通信を行って利用機１００２の認証と識別を行う利用機認証手段１００７と、利用機認証手段１００７の動作結果を基に利用機１００２の信頼度がいかなるものであるかの評価を行う利用機評価手段１００８と、暗号化処理を行う暗号処理手段１００９とを備えている。

【０１４６】また、プロキシ装置１００３は、ＩＣカード１００１に対応して、暗号化処理を行う暗号処理手段１０１０と、利用機１００２の信頼度評価を行う利用機評価手段１０１１とを備えている。ＩＣカード１００１の暗号処理手段１００９とプロキシ装置１００３の暗号処理手段１０１０は対になって情報秘匿を行い、両者間にセキュアパス１０１２を形成する。セキュアパス１０１２形成についての処理手順は第５実施形態と同様であり、詳細説明は省略する。

【０１４７】図１１は本実施形態における利用機の信頼度評価処理の流れを示したフローチャートであり、図１０と合わせて以下その動作を説明する。ここでは、ＩＣカード１００１とプロキシ装置１００３が利用機１００２の信頼度評価結果を共有する場合の処理を例示する。

【０１４８】まず、ＩＣカード１００１の利用機認証手段１００７が利用機１００２の認証もしくは識別を行い、利用機１００２が何者であるかを特定する（ステップ１１０１）。その際、利用機１００２の固有情報を得てＩＣカード１００１が保持する情報と照らし合わせて認証を行う方法、またはＩＣカード１００１と利用機１００２の間で通信を行い、パスワード情報等をやり取りして認証を行う方法等が挙げられるが、基本的に識別及び認証の方法には依存するものではない。既知の技術をもって利用機の識別及び認証を実施可能である。

【０１４９】そして、利用機認証結果を基に、利用機評価手段１００８が利用機の信頼度を評価し、利用機１００２が予め定めたセキュリティポリシ上の分類に基づいてどの程度の信頼度であるのかを算出する（ステップ１００３）。例えば、利用機の信頼度のカテゴリを３段階に分け、「完全に安全」「ほぼ安全」「安全でない」と評価する例で考えると、利用機評価手段１００８はこの３つの状態を数値等の識別可能なデータをもって利用機評価結果とする。さらに具体的な細分化の例として、「利用機運用者による不正行為の可能性」「通りがかりの人間による不正行為の可能性」「ネットワーク経由の不正行為の可能性」をそれぞれ予測して、各項目の有無のマトリクスにより利用機を細かいカテゴリに分類する方法が挙げられる。この場合、それぞれの不正行為の可能性有無によって、いかなる脅威が存在するかを想定することが可能であり、その想定を基にセキュリティポリシを立てれば良い。

【０１５０】次に、セキュアパス１０１２を用いて、ＩＣカード１００１はプロキシ装置１００３に利用機評価結果を渡し（ステップ１１０４）、プロキシ装置１００３が持つ利用機評価手段１０１１がこれを受けて、ＩＣカード１００１が持つ利用機評価手段１００８と利用機１００２の信頼度評価結果を共有する。その後、プロキシ装置１００３は信頼度評価結果に基づいて予め定めた規則に従って通信内容等を設定し、利用機１００２との通信を行う。同様にリモートホスト１００４との通信も行うが、本実施形態においては必ずしもリモートホスト１００４は必要としない。なお、利用機評価手段１００８が獲得する利用機評価結果のデータは、上記の例に限らず様々な形態で実施しうる。

【０１５１】このように、第１３実施形態では、利用機１００２を認証もしくは識別した結果から利用機１００２の信頼度を評価し、その結果をＩＣカード１００１からプロキシ装置１００３にセキュアパス１０１２を介して渡すことにより、利用機１００２の信頼度をＩＣカード１００１とプロキシ装置１００３の両者が共有することができ、利用機１００２やリモートホスト１００４に対するその後の通信に反映させることができる。これは主に、ＩＣカード１００１もしくはプロキシ装置１００３が、不用意に渡してはならない情報を利用機１００２に漏らしてしまうことを防止する作用に反映させることができ、信頼度に応じたセキュリティを確保した適切な情報の送受信が可能となり、その実用的効果は大きい。

【０１５２】［第１４実施形態］図１２は本発明の第１４実施形態に係るＩＣカードシステムの構成を示すブロック図である。第１４実施形態は第１３実施形態の変形例であり、プロキシ装置側に利用機認証手段等を設けたものである。図１２の各構成要素において、符号１２０１～１２０６は図１０における１００１～１００６に、符号１２０９～１２１１は図１０における１００９～１０１１にそれぞれ対応している。

【０１５３】第１３実施形態と異なるのは、プロキシ装置１２０３に利用機認証手段１２０７と利用機評価手段１２０８が設けられることであり、利用機認証結果共有時のデータの流れが第１３実施形態と逆方向になる。図１３は本実施形態における利用機の信頼度評価処理の流

れを示したフローチャートである。この図１３のステップ１３０１～１３０４において、ＩＣカードと利用機の役割が入れ替わる他は、図１１のステップ１１０１～１１０４と処理手順は同様である。

【０１５４】このように、プロキシ装置１２０３が利用機１２０２を認証、識別し、信頼度の評価結果をＩＣカード１２０１に渡すことにより、第１３実施形態と同様に、信頼度の情報をプロキシ装置とＩＣカードで共有することが可能となる。ただし、第１４実施形態においてはプロキシ装置１２０３が利用機１２０２を認証することができ、ＩＣカード１２０１が認証する場合と比較して強力かつ綿密な認証、識別及び信頼度評価が可能となるため、より一層セキュリティの強化を図ることができ、その実用的効果は大きい。

【０１５５】［第１５実施形態］第１５実施形態は、第１４実施形態のさらなる変形例を示したものである。ＩＣカードシステムの構成及び処理の流れはそれぞれ図１２及び図１３と同様である。第１５実施形態では、プロキシ装置１２０３の利用機認証手段１２０７がステップ１３０１で利用機１２０２を認証する際に、計算機ネットワーク１２０５における利用機１２０２の固有情報を用いる。例えば、計算機ネットワーク１２０５がインターネット等のＴＣＰ／ＩＰを通信プロトコルとして用いるネットワークの場合、前記固有情報としてＩＰアドレスが利用できる。利用機認証手段１２０７は、利用機１２０２のＩＰアドレスを元に認証、識別を行う。

【０１５６】このように、第１５実施形態では、計算機ネットワーク１２０５に関連する利用機１２０２の固有情報を用いることにより、利用機の認証や識別が容易にかつ確実にでき、所望のセキュリティを確保したＩＣカードシステムの運用が簡便に実現可能であるため、その実用的効果は大きい。

【０１５７】［第１６実施形態］図１４は本発明の第１６実施形態に係るＩＣカードシステムの構成を示すブロック図である。第１６実施形態は、前述した第１３実施形態に要素を追加した形で構成される。

【０１５８】すなわち、第１３実施形態と同様に、ＩＣカード１４０１、利用機１４０２、プロキシ装置１４０３、リモートホスト１４０４を有して構成され、利用機１４０２とプロキシ装置１４０３、及びプロキシ装置１４０３とリモートホスト１４０４はそれぞれ計算機ネットワーク１４０５を介して接続される。そして、ＩＣカード１４０１は利用機認証手段１４０７、利用機評価手段１４０８及び暗号処理手段１４０９を備え、プロキシ装置１４０３は利用機認証手段１４１２、利用機評価手段１４１３及び暗号処理手段１４１０を備えており、暗号処理手段１４０９と１４１０との間でセキュアパス１４１１を形成する。なお、図に示した例では利用機認証手段は１４０７と１４１２の２つが存在するが、これらは少なくとも片方が備えられていれば良い。

【０１５９】また、ＩＣカード１４０１は送信情報制御手段１４１４を備え、この送信情報制御手段１４１４により、利用機評価手段１４０８の動作結果を基にしてＩＣカード１４０１から利用機１４０２に送信するデータ内容を制御する。すなわち、利用機１４０２の信頼度の高低に応じて、もしくは第１３実施形態で示したように信頼度の要素がマトリクス上に細分化されている場合は個々のセキュリティポリシに照らして、適切なデータを送信する。その最も単純な例は、利用機評価結果を「信頼できる」「信頼できない」の２値とし、「信頼できない」場合には「機密」に分類されたデータを一切送信しないことである。

【０１６０】このように、第１６実施形態では、ＩＣカード１４０１の利用機評価手段１４０８の動作結果を用いて送信情報制御手段１４１４が利用機１４０２の信頼度に応じたデータを送信することにより、柔軟かつ強力なセキュリティを得ることができ、その実用的効果は大きい。この場合、ＩＣカード側で信頼度を判断して送信データの内容を制御することが可能である。

【０１６１】［第１７実施形態］第１７実施形態は前述した第１６実施形態の送信情報制御に関する第１の例であり、ＩＣカードシステムの構成は図１４と同様である。第１７実施形態では、利用機評価手段１４０８の動作結果を基に利用機１４０２の信頼度の高低を評価した結果が「信頼できない」と判断される場合に、ＩＣカード１４０１のアプリケーションが利用機１４０２に送信しようとしていたデータについて、送信前に送信情報制御手段１４１４が処理し、セキュリティポリシ上利用機１４０２に対して漏らすべきでない情報を削除する。これにより、利用機１４０２毎の信頼度に応じた情報秘匿が可能となる。なお、信頼度評価結果を多値とし、各々の信頼度の値に従って異なる方法でデータから情報の一部もしくは全部を削除する方法でも同様に実施可能である。

【０１６２】［第１８実施形態］第１８実施形態は前述した第１６実施形態の送信情報制御に関する第２の例であり、ＩＣカードシステムの構成は図１４と同様である。第１８実施形態では、送信情報制御手段１４１４は、ＩＣカード１４０１が保持する機密情報を送信前にチェックし、利用機評価手段１４０８が利用機１４０２を「信頼できない」と判断した場合には、機密情報を送信データから削除もしくは他のデータに変更する。これにより、ＩＣカード１４０１が保持する機密情報の秘匿を利用機１４０２毎の信頼度に応じて行うことが可能となる。

【０１６３】［第１９実施形態］第１９実施形態は前述した第１６実施形態の送信情報制御に関する第３の例であり、ＩＣカードシステムの構成は図１４と同様である。第１９実施形態では、送信情報制御手段１４１４は、ＩＣカード１４０１が保持するＩＣカード１４０１

のユーザのプライバシに関わる情報を送信前にチェックし、利用機評価手段１４０８が利用機１４０２を「信頼できない」と判断した場合には、プライバシ情報を送信データから削除もしくは他のデータに変更する。これにより、ＩＣカード１４０１が保持するプライバシ情報の秘匿を利用機１４０２毎の信頼度に応じて行うことが可能となる。

【０１６４】［第２０実施形態］図１５は本発明の第２０実施形態に係るＩＣカードシステムの構成を示すブロック図である。第２０実施形態は、前述した第１４実施形態に要素を追加した形で構成される。

【０１６５】すなわち、第１４実施形態と同様に、ＩＣカード１５０１、利用機１５０２、プロキシ装置１５０３、リモートホスト１５０４を有して構成され、利用機１５０２とプロキシ装置１５０３、及びプロキシ装置１５０３とリモートホスト１５０４はそれぞれ計算機ネットワーク１５０５を介して接続される。そして、ＩＣカード１５０１は利用機認証手段１５０７、利用機評価手段１５０８及び暗号処理手段１５０９を備え、プロキシ装置１５０３は利用機認証手段１５１２、利用機評価手段１５１３及び暗号処理手段１５１０を備えており、暗号処理手段１５０９と１５１０との間でセキュアパス１５１１を形成する。なお、図に示した例では利用機認証手段は１５０７と１５１２の２つが存在するが、これらは少なくとも片方が備えられていれば良い。

【０１６６】この第２０実施形態は、第１６実施形態と比較した場合、送信情報制御手段１５１４をＩＣカード１５０１ではなくプロキシ装置１５０３側に設けた点が構成上異なる。この送信情報制御手段１５１４により、利用機評価手段１５１３の動作結果を基にしてプロキシ装置１５０３から利用機１５０２に送信するデータ内容を制御する。すなわち、利用機１５０２の信頼度の高低に応じて、セキュリティポリシ上好ましい状態のデータを送信する。

【０１６７】このように、第２０実施形態では、第１６実施形態と同様に、プロキシ装置１５０３の利用機評価手段１５１３の動作結果を用いて送信情報制御手段１５１４が利用機１５０２の信頼度に応じたデータを送信することにより、柔軟かつ強力なセキュリティを得ることができ、その実用的効果は大きい。この場合、ＩＣカード側で利用機の信頼度がわからなくても、プロキシ装置側で信頼度を判断して送信データの内容を制御することが可能である。

【０１６８】［第２１実施形態］第２１実施形態は前述した第２０実施形態の送信情報制御に関する第１の例であり、ＩＣカードシステムの構成は図１５と同様である。第２１実施形態では、利用機評価手段１５１３の動作結果を基に利用機１５０２の信頼度の高低を評価した結果が「信頼できない」と判断される場合に、プロキシ装置１５０３のアプリケーションが利用機１５０２に送信しようとしていたデータについて、送信前に送信情報制御手段１５１４が処理し、セキュリティポリシ上利用機１５０２に対して漏らすべきでない情報を削除する。これにより、利用機１５０２毎の信頼度に応じた情報秘匿が可能となる。なお、信頼度評価結果を多値とし、各々の信頼度の値に従って異なる方法でデータから情報の一部もしくは全部を削除する方法でも同様に実施可能である。

【０１６９】［第２２実施形態］第２２実施形態は前述した第２０実施形態の送信情報制御に関する第２の例であり、ＩＣカードシステムの構成は図１５と同様である。第２２実施形態では、送信情報制御手段１５１４は、プロキシ装置１５０３が保持する機密情報を送信前にチェックし、利用機評価手段１５１３が利用機１５０２を「信頼できない」と判断した場合には、機密情報を送信データから削除もしくは他のデータに変更する。これにより、プロキシ装置１５０３が保持する機密情報の秘匿を利用機１５０２毎の信頼度に応じて行うことが可能となる。

【０１７０】［第２３実施形態］第２３実施形態は前述した第２０実施形態の送信情報制御に関する第３の例であり、ＩＣカードシステムの構成は図１５と同様である。第２３実施形態では、送信情報制御手段１５１４は、プロキシ装置１５０３が保持するＩＣカード１５０１のユーザのプライバシに関わる情報を送信前にチェックし、利用機評価手段１５１３が利用機１５０２を「信頼できない」と判断した場合には、プライバシ情報を送信データから削除もしくは他のデータに変更する。これにより、プロキシ装置１５０３が保持するＩＣカードユーザのプライバシ情報の秘匿を利用機１５０２毎の信頼度に応じて行うことが可能となる。

【０１７１】［第２４実施形態］図１６は本発明の第２４実施形態に係るＩＣカードシステムの構成を示すブロック図である。第２４実施形態は、第１実施形態と同様に、ＩＣカード１６０１、利用機１６０２、プロキシ装置１６０３、リモートホスト１６０４を有して構成され、利用機１６０２とプロキシ装置１６０３、及びプロキシ装置１６０３とリモートホスト１６０４はそれぞれ計算機ネットワーク１６０５を介して接続される。利用機１６０２はＩＣカードリーダライタ１６０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０１７２】ＩＣカード１６０１は利用機認証手段１６０７、利用機評価手段１６０８、暗号処理手段１６０９を、プロキシ装置１６０３は利用機認証手段１６１２、利用機評価手段１６１３、暗号処理手段１６１０をそれぞれ備えており、暗号処理手段１６０９と１６１０との間でセキュアパス１６１１を形成する。これらの手段の基本的構成は前述した第１３、第１４、第１６、及び第２０実施形態と同様である。

【０１７３】また、ＩＣカード１６０１はＵＩリクエスト情報送信手段１６１５を備え、プロキシ装置１６０３はＵＩリクエスト情報受信手段１６１６とＵＩ情報送信手段１６１７を備え、利用機１６０２はＵＩ情報受信手段１６１８とＵＩ実行手段１６１９を備えている。これらの手段の基本的構成は前述した第９及び第１０実施形態と同様である。

【０１７４】さらに、本実施形態では、プロキシ装置１６０３は送信情報制御手段１６１４を備えている。利用機評価手段１６１３により得られる利用機１６０２の信頼度に応じて、ＵＩ情報送信手段１６１７が利用機１６０２のＵＩ情報受信手段１６１８にデータを送る前に、信頼度が低い場合は送信情報制御手段１６１４が作用してデータの変更、制限を行う。

【０１７５】図１７は本実施形態におけるＵＩ実行処理の流れを示したフローチャートであり、図１６と合わせて以下その動作を説明する。まず、ＩＣカード１６０１とプロキシ装置１６０３が利用機１６０２の信頼度情報を共有する（ステップ１７０１、ステップ１７０２）。この信頼度情報共有のための処理手順は第１３及び第１４実施形態に示した通りである。そして、ＩＣカード１６０１に搭載したアプリケーションが生成したＵＩリクエスト情報を送信し、これをプロキシ装置１６０３が受け取り、それを基にＵＩ情報を生成する（ステップ１７０３～１７０６）。この間の処理手順は第９実施形態に示した通りである。

【０１７６】次に、プロキシ装置１６０３の利用機評価手段１６１３が、利用機１６０２の信頼度を評価する（ステップ１７０７）。ここでは、信頼度評価結果の例として「信頼できる」「信頼できない」の２値評価を適用する。「信頼できる」と評価した場合は、生成されたＵＩ情報をそのまま利用機１６０２に送信する（ステップ１７０９）。一方、「信頼できない」と評価した場合は、ステップ１７０９に進む前に、送信情報制御手段１６０４がＵＩ情報に変更を加え、ユーザインタフェースに制限を掛け（ステップ１７０８）、その後ステップ１７０９に進む。

【０１７７】そして、利用機１６０２は受信したＵＩ情報を基にＵＩ実行のための情報を形成し、具備しているハードウェアを駆動してＵＩを実行する（ステップ１７１０～１７１２）。このステップ１７０９～１７１２に至る処理手順は第９実施形態に示した通りである。

【０１７８】図１８はＵＩリクエスト情報の一例を示す動作説明図である。この例では、ＵＩリクエスト情報１８００は、表示コマンド１８０１と表示属性１８０２及び表示対象配列１８０３の３種類のデータの複合情報から成る。表示コマンド１８０１はＵＩリクエスト情報１８０１の求めるＵＩ動作を識別するためのデータであり、表示属性１８０２は表示位置、文字指定、文字属性その他の表示に関わる情報を含んだデータである。表示対象配列１８０３は表示する対象となるデータを特定するための情報を複数収めた配列データである。

【０１７９】表示対象配列１８０３の各要素として、この例ではユーザ氏名情報１８０４、住所情報１８０５、電話番号情報１８０６、勤務先情報１８０７、口座番号情報１８０８、口座残高情報１８０９、取引履歴情報１８１０を格納する。これらの各要素情報１８０４～１８１０には、例えば氏名であれば氏名を表現した文字列データそのものを入れても良いし、またはプロキシ装置１６０３が氏名の文字列を得ることができるような識別情報を入れても良い。ただし、この情報が氏名に関わるものであることを、プロキシ装置１６０３が認識できるための情報が含められている必要がある。

【０１８０】なお、これらのＵＩリクエスト情報のデータ構造はあくまで一例であり、他の様々な方法によって類似する情報内容を構成し得る。

【０１８１】上記のＵＩリクエスト情報１８００を、図１７に示したステップ１７０４～１７０５でＩＣカード１６０１からプロキシ装置１６０３に伝送する際、原則としてセキュアパス１６１１を介するのが好ましい。ただし、ＵＩリクエスト情報に含まれる情報から機密に関わる情報を直接もしくは間接的に利用機１６０２が得ることができないことが分かっている場合は、セキュアパス１６１１以外の手段を用いて伝送しても良い。

【０１８２】図１９は、ＵＩ情報及びＵＩ実行結果の第１の例として、利用機が「信頼できる」と評価された場合を示す動作説明図である。これは、プロキシ装置１６０３の利用機評価手段１６１３が、図１７のステップ１７０７において利用機１６０２を「信頼できる」と評価した場合である。

【０１８３】図１９（Ａ）に示すＵＩ情報１９０１は、上述したように図１７のステップ１７０６にて生成される。ＵＩ情報１９０１の内容は、個々の表示対象に対して、それが文字表示であることを表すコマンド情報１９０２、表示時の詳細な制御内容（表示属性）を表す属性情報１９０３を、それぞれ表示対象データ１９０４～１９１０と組にして一まとめにしたものである。表示対象データ１９０４～１９１０には、例えば氏名であれば氏名を表す文字列情報が直接含まれ、それらは文字コードもしくは文字を表現する画像データから構成される。

【０１８４】このＵＩ情報１９０１は、利用機１６０２のＵＩ実行手段１６１９によって解釈されるデータもしくはプログラムとして扱うことができる。なお、ＵＩ情報に関してもＵＩリクエスト情報と同じく、本実施形態で挙げた例の他に様々な方法によって構成し得る。

【０１８５】この第１の例のように、利用機１６０２が「信頼できる」場合、ＵＩ実行結果は図１９（Ｂ）に示すようになる。すなわち、表示対象データ１９０４～１９１０に対応する全てのデータ内容が、ＵＩ実行結果１９１１として利用機１６０２の表示画面装置等に表示出

力される。

【０１８６】図２０は、ＵＩ情報及びＵＩ実行結果の第２の例として、利用機が「信頼できない」と評価された場合を示す動作説明図である。これは、プロキシ装置１６０３の利用機評価手段１６１３が、図１７のステップ１７０７において利用機１６０２を「信頼できない」と評価した場合である。

【０１８７】この場合、ステップ１７０８で送信情報制御手段１６１４が作用し、図２０（Ａ）に示すＵＩ情報２００１のように、機密に関わる表示対象データである口座番号データ１９０８、口座残高データ１９０９、取引履歴データ１９１０を、それぞれダミーデータ２００２～２００４に書き換える。

【０１８８】この第２の例では、図２０（Ｂ）に示すように、ＵＩ実行結果２００５は機密に関わる個々のデータはダミーデータとして「Ｘ」などに置き換えられ、隠匿された状態で利用機１６０２の表示画面装置等に表現されるので、画面表示内容を搾取されたり印刷内容を盗用されたりした場合でも、機密が漏洩することを防げる。また、ＵＩ情報２００１そのものにもこれらの機密情報が含まれていないため、不正な手段を用いてＵＩ情報を解析したとしても、機密の漏洩を防止できる。

【０１８９】なお、本実施形態では、利用機評価手段１６１３による信頼度評価を２値評価とした例で説明したが、評価結果を細分化して多値評価を行い、それに応じてステップ１７０８における処理を多岐に分ける方法を採っても実施可能である。これをＵＩ情報及びＵＩ実行結果の第３の例として、上記第２の例とは異なる条件での機密管理の実行例を図２１に示す。

【０１９０】図２１は、ＵＩ情報及びＵＩ実行結果の第３の例として、利用機が「さらに信頼できない」と評価された場合を示す動作説明図である。この第３の例では、図２０の場合よりも「さらに信頼できない」利用機を想定しており、ＵＩ情報２１０１は、口座に関する情報はもとより、ユーザの住所、電話番号、勤務先情報まで機密としてダミーデータに書き換え、利用機１６０２に漏洩しないようにしている。この場合のＵＩ実行結果２１０２は、ユーザの氏名情報以外は全てダミーデータとして「Ｘ」などに置き換えられて利用機１６０２の表示画面装置等に表示される。

【０１９１】このように、利用機評価手段１６１３の評価結果に基づいて利用機１６０２上で実行されるＵＩに変更を掛けて表示する情報を制限することにより、利用機１６０２の信頼度が低い場合に、表示画面装置等に表現された情報が搾取されたりしても機密情報を盗み取られるおそれがなくなり、その実用的効果は極めて高い。この第２４実施形態によって、［発明が解決しようとする課題］の欄に示した第２の問題点のうち、画面出力、印刷出力等のユーザへの出力内容から機密が漏洩する問題を明確に解決することができる。

【０１９２】［第２５実施形態］第２５実施形態はＵＩ制御処理の他の例を示したものである。ＩＣカードシステムの構成と処理の流れは第２４実施形態と同様である。この実施形態は、ＵＩ実行の内容が表示ではなく、入力に関わる点が第２４実施形態と異なる。

【０１９３】図２２はＵＩリクエスト情報及びＵＩ実行結果の例を示す動作説明図である。図２２（Ａ）に示すように、ＵＩリクエスト情報２２０１は、文字入力を促すＵＩを得るための入力コマンド情報２２０２、文字入力に関する属性情報２２０３、入力対象要素であるユーザ名２２０５及びパスワード２２０６からなる入力対象配列２２０４、入力ボタンのＵＩを得るためのボタンコマンド情報２２０７、ボタンに関する属性情報２２０８、ボタン要素である公開情報２２１０及び秘密情報２２１１からなるボタン配列２２０９を含んでいる。このＵＩリクエスト情報２２０１は、ユーザ名、パスワードを入力する２つの文字入力フィールドと、公開情報、秘密情報を得るための２つのボタンを入力部品としたＵＩを利用機１６０２上で実行することを要求するものである。

【０１９４】このＵＩリクエスト情報２２０１に対して第２４実施形態と同様の処理を行い、利用機１６０２の信頼度評価結果に応じて異なるＵＩ情報を用意する。ここで、利用機１６０２が「信頼できる」場合は図２２（Ｂ）に示すようなＵＩ実行結果２２１２が、「信頼できない」場合は図２２（Ｃ）に示すようなＵＩ実行結果２２１３がそれぞれ得られる。すなわち、「信頼できる」場合は要求された全ての入力部品が利用機１６０２上で実行されて表示され、「信頼できない」場合はパスワード入力フィールド及び秘密情報ボタンがＵＩの表示から削除される。

【０１９５】これにより、利用機１６０２の信頼度が低い場合は機密情報入力用のＵＩが表示されないため、ユーザは機密に関わる情報を利用機１６０２上の機器を用いて入力することができなくなり、機密情報の漏洩が防止できる。特に、パスワード入力についてはキー入力の状態を搾取することによるパスワード盗用を防ぐことが可能であり、その実用的効果は極めて大きい。

【０１９６】次に、第２４実施形態と第２５実施形態を複合的に適用したウェブメール、即ちＷＷＷの仕組みを利用した個人向け電子メールサービスの具体例を示す。ウェブメールを読むためのＷＷＷブラウザに相当するアプリケーションをＩＣカードが持ち、このアプリケーションは利用機を通じてウェブメールサーバ（ウェブメールサービスを行うリモートホスト）にアクセスする。この時、第２実施形態及び第４実施形態に示したアクセス先情報秘匿を適用すれば、利用機に対してウェブメールサーバの所在を隠すこともできる。

【０１９７】ＩＣカードのアプリケーションは、ウェブメールサーバからＩＣカードユーザの受信メール一覧を

取得し、ＵＩリクエスト情報をプロキシ装置に送る。プロキシ装置はＵＩリクエスト情報に基づいてＵＩ情報を構築するが、その際利用機評価手段の作用によって利用機を「信頼できる」と判断した場合はＵＩ情報には全ての受信メールの見出し情報と、メール本文を読むためのボタン（WWWのリンク）を含んだままとする。一方、利用機を「信頼できない」と判断した場合には、受信メールのうち機密と分類されるものについての見出し情報を隠し（あるいは他の非機密情報に変更し）、さらにメール本文を読むためのボタンも含まないようにする。

【０１９８】図２３は「信頼できる」利用機を使用した場合のＵＩ実行結果の一例を、図２４は「信頼できない」利用機を使用した場合のＵＩ実行結果の一例をそれぞれ示したものである。

【０１９９】図２３に示すように、信頼できる利用機の場合は、全ての受信メールの差出人、送信日時及びサブジェクト（メールのタイトル）が表示され、さらにそれらがWWWのリンクとなり、ユーザはそのリンクを指定する（タッチパネルでクリックもしくはポインティングデバイスでリンクの場所にポインタを合わせてボタン等で指定する）ことで、それらのメールの本文を読むことができる。しかし、図２４に示すように、信頼できない利用機の場合は、例えばサブジェクトに「機密」もしくは「SECRET」という文字列が含まれるメールを全て機密文書とみなし、そのメールに関する一切の情報を表示させないようにしている。もちろん本文も読むことはできない。

【０２００】上記の例では、機密文書の判断基準として単純にサブジェクトに含まれる文字列のみを用いたが、他に、差出人による判断、メールのヘッダよる判断、もしくはメール本文を先に（利用機に表示することなく）解析して機密にあたる情報が含まれるか否かを判断する等の方法が考えられる。また、上記の例ではWWWブラウザに相当するアプリケーションをＩＣカードに搭載するようにしたが、これを利用機に持たせ、ＩＣカードはプロキシ装置と連携してウェブメールサーバから得る情報に制限を加える方法でも実施可能である。

【０２０１】いずれにしても、本実施形態によって、［発明が解決しようとする課題］の欄に示した第２の問題点を明確に解決することができる。本実施形態では機密情報の入力そのものを不可とするため、暗証番号やパスワードを要求するリモートホストのサービスは受けることができないが、機密情報漏洩に対しては強力な効果を発揮するものである。

【０２０２】［第２６実施形態］図２５は本発明の第２６実施形態に係るＩＣカードシステムの構成を示すブロック図である。第２６実施形態は、第１実施形態と同様に、ＩＣカード２５０１、利用機２５０２、プロキシ装置２５０３、リモートホスト２５０４を有して構成され、利用機２５０２とプロキシ装置２５０３、及びプロキシ装置２５０３とリモートホスト２５０４はそれぞれ計算機ネットワーク２５０５を介して接続される。利用機２５０２はＩＣカードリーダライタ２５０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０２０３】ＩＣカード２５０１は、利用機を通じてユーザが入力したデータ（仮の機密情報）を基に、別のデータ（真の機密情報）を生成する機密情報変換手段２５０７を備える。また、図示しないが、ＩＣカード２５０１およびプロキシ装置２５０３はそれぞれ暗号処理手段を備えており、これらの暗号処理手段と利用機２５０３が持つデータ転送手段との組み合わせでセキュリティを確保したデータ通信経路としてセキュアパス２５０８が形成される。このセキュアパス２５０８は前述した実施形態と同様であり、ここでは説明を省略する。なお、機密情報変換手段２５０７は、ＩＣカード２５０１ではなくプロキシ装置２５０３が備える構成としても良い。その場合にはセキュアパス２５０８は不要である。

【０２０４】利用機２５０２はＵＩ実行手段２５０９を備えている。このＵＩ実行手段２５０９は、前述の第９～第２５実施形態で示したものの他、利用機２５０２自身の処理作用による一般的なＵＩも含むことができる。プロキシ装置２５０３は、ＩＣカード２５０１の機密情報変換手段２５０７から機密情報を受け取る機密情報獲得手段２５１０を備えている。なお、この機密情報獲得手段２５０７をプロキシ装置２５０３が備える場合には、機密情報変換手段２５０７と一体化しても良い。

【０２０５】リモートホスト２５０４は機密情報要求手段２５１１を備えている。この機密情報要求手段２５１１は、リモートホスト２５０４が提供するサービスにおいて暗証番号やパスワードの入力を要求する一般的な事物を表す。ここで、機密情報要求手段２５１１が求める情報を、真の機密情報と呼ぶことにする。即ち、リモートホスト２５０４のサービスを利用しようとする者は、真の機密情報を機密情報要求手段２５１１に渡すことで、初めて利用のための権限が与えられる。

【０２０６】図２６は本実施形態における機密情報保護処理の流れを示したフローチャートであり、図２５と合わせて以下その動作を説明する。まず、ＩＣカード２５０１のユーザは、利用機２５０２のＵＩ実行手段２５０９を用いて真の機密情報を得るためのキーとなる情報を入力する（ステップ２６０１）。以下、この情報を仮の機密情報と呼ぶことにする。なお、仮の機密情報そのものには機密性はなく、これを搾取してリモートホスト２５０４のサービスを受けることはできないようになっている。次に、利用機２５０２は仮の機密情報をＩＣカード２５０１に送信し、ＩＣカード２５０１はこれを受信する（ステップ２６０２、ステップ２６０３）。ＩＣカード２５０１の機密情報変換手段２５０７は、受信した仮の機密情報を元に演算を行い、真の機密情報を生成す

る（ステップ２６０４）。

【０２０７】仮の機密情報から真の機密情報を生成する方法の例としては、予め定めたキーワード（合い言葉）を仮の機密情報とし、ユーザが入力したキーワードから、それに対応する情報を登録済みの情報から検索して真の機密情報とする方法、あるいは予め定めた変換方法に従って真の機密情報を変換したものを仮の機密情報として、ユーザが入力したデータに逆変換を掛けて真の機密情報を得る方法、等が挙げられる。前者はユーザが覚えやすいキーワードを用いることで使用が簡単になる反面、予め登録しておかなかった真の機密情報は扱えないという特徴がある。後者は任意の情報を生成することが容易であり、特に文字列による機密情報の入力を行う際に適するが、その反面、変換規則をユーザが把握し、自ら何らかの手段を用いて変換データを用意する必要があり、難解になり易い特徴がある。また、いずれの場合にも仮の機密情報から真の機密情報を容易に類推されないことが重要である。

【０２０８】機密情報変換手段２５０７で真の機密情報を生成した後、ＩＣカード２５０１はセキュアパス２５０８を通じて真の機密情報をプロキシ装置２５０３の機密情報獲得手段２５１０に渡す（ステップ２６０５、ステップ２６０６）。最後に、プロキシ装置２５０３は真の機密情報をリモートホスト２５０４の機密情報要求手段２５１１に渡す（ステップ２６０７）。

【０２０９】なお、機密情報変換手段２５０７をプロキシ装置２５０３が備える場合には、上記のステップ２６０２において仮の機密情報は利用機２５０２からプロキシ装置２５０３に渡され、ステップ２６０３及びステップ２６０４の機密情報変換はプロキシ装置２５０３内で処理される。またこの場合、ステップ２６０５とステップ２６０６は不要となり、プロキシ装置２５０３はステップ２６０４にて生成した真の機密情報をそのままステップ２６０７にてリモートホスト２５０４に渡せば良い。

【０２１０】図２７は、本実施形態を適用したＵＩ実行結果であるパスワード入力ＵＩの画面例と、パスワード情報としてリモートホストに渡されるデータの具体例を示した動作説明図である。図２７において、（Ａ）は利用機上に表示されるＵＩ画面表示例、（Ｂ）は仮の機密情報をパスワードとして入力した状態のＵＩ画面表示例、（Ｃ）は真の機密情報と仮の機密情報の一例をそれぞれ示す。この場合、ユーザからは真の機密情報（正パスワード）である文字列“mYReALpassWORd”の代わりに、仮の機密情報（仮パスワード）である文字列“temppasswd1”が利用機２５０２に与えられる。そして、文字列“temppasswd1”は機密情報変換手段２５０７によって文字列“mYReALpassWORd”に変換され、パスワードとしてリモートホスト２５０４に渡される。

【０２１１】このように、第２６実施形態では、機密情報をユーザが直接に利用機２５０２に与える代わりに仮の機密情報を入力し、それをＩＣカード２５０１の機密情報変換手段２５０７で真の機密情報に変換してセキュアパス２５０８を通じてプロキシ装置２５０３に渡すことで、機密方法を利用機２５０２に秘匿した状態でリモートホスト２５０４へ渡すことができる。即ち、ウェブメール、オンラインショッピング等、アクセスパスワードの入力が必要なサービスを、ＩＣカードのユーザが利用機にパスワードを漏洩させることなく利用することが可能となり、その実用的効果は極めて大きい。この実施形態によって、［発明が解決しようとする課題］の欄に示した第２の問題点のうち、キーボード、タッチパネル等の入力手段によるユーザからの入力内容から機密が漏洩する問題を明確に解決することができる。また、第２６実施形態では、第２５実施形態のように機密情報を秘匿するものとは異なり、機密情報を変換して受け渡すことで暗証番号やパスワードを要求するリモートホストのサービスを受けることが可能である。

【０２１２】［第２７実施形態］第２７実施形態は前述した第２６実施形態の機密情報保護に関する第１の変形例であり、ＩＣカードシステムの構成及び処理の流れは第２６実施形態と基本的に同様である。この例は、機密情報変換手段２５０７が行う変換処理のためのデータを、ユーザによる仮の機密情報入力に先立って装置からユーザに提示する点が異なる。

【０２１３】図２８はＵＩ実行結果として利用機上に表示されるＵＩ画面とそこに情報を入力した状態の具体例を示す動作説明図である。この場合、利用機２５０２のＵＩ実行手段２５０９によってパスワード入力に関する情報がユーザに提示され、それを受けてユーザが仮の機密情報である仮パスワードを入力する。パスワードを入力するＵＩ部品には、パスワード入力領域に付随して、変換キーを表示する領域を設ける。変換キーは機密情報変換手段２５０７が変換処理に使用するパラメータであり、変換キーが違えば真の機密情報として同一の結果を得るための仮の機密情報は異なるように、変換キー毎に仮の機密情報を設定する必要がある。ここでは変換キーとして“１２”という数字を用いているが、この数字はユーザが利用機を使用する毎に異なる値にすることが必要で、乱数を用いることが望ましい。

【０２１４】ユーザは、図２６に示したステップ２６０１において、変換キーの内容を考慮して、真の機密情報に正しく変換される文字列を仮の機密情報として入力する。それ以降の処理は第２６実施形態と同様である。ただし、この場合、ステップ２６０４において機密情報変換手段２５０７が真の機密情報を生成する際に、ユーザに提示した変換キーと同一のデータを用いて変換処理を行うことが必須である。このようなランダムデータを用いた機密情報の入力は、動的認証（ダイナミックオーセンティケーション）技術として一般に知られているが、

本実施形態は、機密情報を要求するリモートホスト２５０４が動的認証を行わない場合においても適用可能である点と、ランダムデータの提示を含むＵＩを、第９～第２５実施形態で示したＵＩ情報の形成方法を用いてプロキシ装置２５０３が行うことによって、ユーザにランダムデータを提示するための特別な仕組を利用機２５０２に持たせることなく実現可能である点に特徴がある。

【０２１５】このように第２７実施形態では、機密情報変換手段２５０７が都度生成するランダムデータを、ＵＩ実行手段２５０９を通じて変換キーとしてユーザに提示し、ユーザから入力された仮の機密情報を同一の変換キーを用いて変換処理を行うことにより、ユーザからの直接入力される内容を毎回異なるものにすることが可能となる。仮の機密情報から真の機密情報が類推されることを防ぐ場合、毎回同じデータを与えるよりも乱数による異なるデータを与えた方がより機密性が高まるため、本実施形態がもたらすセキュリティ向上の実用的効果は大きい。

【０２１６】［第２８実施形態］第２８実施形態は前述した第２６実施形態の機密情報保護に関する第２の変形例であり、ＩＣカードシステムの構成及び処理の流れは第２６および第２７実施形態と基本的に同様である。この例は、図２６に示したステップ２６０１において、もしくはステップ２６０１に先立って、ユーザが真の機密情報を誤って入力しないための注意メッセージをＵＩ実行手段２５０９がユーザに提示する点が異なる。この注意メッセージの提示も、第２７実施形態と同様に、第９～第２５実施形態で示したＵＩ情報の形成方法を用いてプロキシ装置２５０３が行うことができる。

【０２１７】図２９はＵＩ実行結果として利用機上に表示されるＵＩ画面とそこに情報を入力した状態の具体例を示す動作説明図である。この場合、利用機２５０２のＵＩ実行手段２５０９によってパスワード入力に関する情報がユーザに提示され、それを受けてユーザが仮の機密情報である仮パスワードを入力する。パスワードを入力するＵＩ部品には、パスワード入力領域、変換キー表示領域に付随して、誤って真の機密情報即ちリモートホスト２５０４の機密情報要求手段２５１１が要求する本当のアクセスパスワード（正パスワード）を入力しないよう、ユーザに注意を促すメッセージを追加している。なお、本実施形態では第２７実施形態に倣う形で変換キーを表示しているが、第２６実施形態に倣う形として変換キーを表示せず、注意メッセージのみを付加しても良い。

【０２１８】このように第２８実施形態では、ＵＩ実行手段２５０９がユーザに注意メッセージを示すことにより、誤って真の機密情報を入力してしまい、機密を漏洩させてしまうトラブルを防ぐ効果を得ることができる。

【０２１９】［第２９実施形態］図３０は本発明の第２９実施形態に係るＩＣカードシステムの構成を示すブロック図である。第２９実施形態は、ＩＣカード３００１、利用機３００２、リモートホスト３００６と共に、計算機ネットワーク３００７上に複数のプロキシ装置３００３～３００５を備えた例である。また、本実施形態では、ＩＣカード３００１はプロキシ選択手段３００８を備える。プロキシ選択手段３００８は、計算機ネットワーク３００７上にある複数のプロキシ装置３００３、３００４、及び３００５の中から、予め定めた規則に従って一つを選択する。選択されたプロキシ装置は前述した第１～第２８実施形態のいずれかに示すプロキシ装置として動作する。

【０２２０】なお、本実施形態ではプロキシ装置の数を３つとしたが、この数は限定的ではなく、実施可能な範囲において制限はない。また、リモートホストも１つとしたが、複数のリモートホストが計算機ネットワーク上に存在しても良い。これは他の実施形態においても同様である。

【０２２１】この第２９実施形態では、計算機ネットワーク３００７上に複数のプロキシ装置を設置し、ＩＣカード３００１にプロキシ選択手段３００８を備えることにより、複数のプロキシ装置を選択的に使用することが可能となり、負荷分散、パフォーマンス最適化及びフォールトトレランス（障害に対する寛容性）の面でその実用的効果は大きい。

【０２２２】［第３０実施形態］第３０実施形態は前述した第２９実施形態のプロキシ装置選択に関する第１の例であり、ＩＣカードシステムの構成は図３０と同様である。第３０実施形態では、ＩＣカード３００１において、プロキシ選択手段３００８はプロキシデータのリストから逐次的にプロキシ装置の情報を読み取り、使用に適するものが発見でき次第それを選択する。図３１にプロキシ選択手段の動作の概念図を例示する。プロキシ装置選択の際に、使用に適するか否かを判断する方法は様々考えられるが、例えば実際に利用機を通じて通信ができるかどうかを調べる方法、通信できた場合に、予め定めたレスポンスタイムを下回ることをさらに条件とする方法等が挙げられる。これにより、比較的単純なアルゴリズムでプロキシ装置を選択することができる。

【０２２３】［第３１実施形態］第３１実施形態は前述した第２９実施形態のプロキシ装置選択に関する第２の例であり、ＩＣカードシステムの構成は図３０と同様である。第３１実施形態では、ＩＣカード３００１において、プロキシ選択手段３００８はプロキシデータのリストからランダムにプロキシ装置の情報を読み取り、第３０実施形態と同様に、使用に適するものが発見でき次第それを選択する。図３２にプロキシ選択手段の動作の概念図を例示する。これにより、より負荷分散性を高めたプロキシ装置選択が可能となる。

【０２２４】［第３２実施形態］第３２実施形態は前述した第２９実施形態のプロキシ装置選択に関する第３の

例であり、ＩＣカードシステムの構成は図３０と同様である。第３２実施形態では、ＩＣカード３００１において、プロキシ選択手段３００８は利用機３００２と通信を行って問い合わせをし、最適なプロキシ装置を選択する。この場合、ＩＣカード３００１よりも高い計算能力を持つ利用機３００２のプロキシ選択処理手段を利用して処理を行うことにより、プロキシ装置選択に関してよりきめ細かく柔軟な最適解を得ることが可能となる。ただし、利用機３００２の信頼度が低い場合、最適なプロキシ装置を偽って選択されたり、不正なプロキシ装置を故意に選択される可能性もあるため、ＩＣカード３００１と選択されたプロキシ装置との間で適切な相互認証が求められる。少なくとも、ＩＣカード３００１によるプロキシ装置の厳格な認証は必要不可欠である。なお、他の実施形態においても、ＩＣカードとプロキシ装置間で相互認証を行うことが望ましい。

【０２２５】［第３３実施形態］第３３実施形態は前述した第２９実施形態のプロキシ装置選択に関する第４の例であり、ＩＣカードシステムの構成は図３０と同様である。第３３実施形態では、第２９実施形態を基本として、図３３に示すようにさらにＩＣカード３００１のプロキシ選択手段３００８が持つプロキシ装置のリストを、ＩＣカードのユーザが追加、変更、削除することができるプロキシ情報操作手段３００９を備える。プロキシ情報操作手段３００９を用いた操作方法の例としては、利用機を通じてプロキシ情報の追加、変更、削除等を行う方法が挙げられるが、その際信頼度の高い利用機を用いることが望ましい。

【０２２６】これにより、ＩＣカードのユーザはプロキシ装置のリストを柔軟に操作することができ、新規のプロキシ装置の追加、プロキシ装置の変更や撤廃等に対して適切な対応を取ることが可能となり、その実用的効果は大きい。

【０２２７】［第３４実施形態］図３４は本発明の第３４実施形態に係るＩＣカードシステムの構成を示すブロック図である。第３４実施形態は、第１実施形態と同様に、ＩＣカード３４０１、利用機３４０２、プロキシ装置３４０３、リモートホスト３４０４を有して構成され、利用機３４０２とプロキシ装置３４０３、及びプロキシ装置３４０３とリモートホスト３４０４はそれぞれ計算機ネットワーク３４０５を介して接続される。利用機３４０２はＩＣカードリーダライタ３４０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０２２８】本実施形態では、ＩＣカード３４０１はインセンティブ発行手段３４０７を、利用機３４０２はインセンティブ獲得手段３４０８をそれぞれ備える。インセンティブ発行手段３４０７は、インセンティブ獲得手段３４０８と通信を行い、利用機及び利用機の所有者や運用者が金銭的、事業的に有利となる状態をもたらすものである。インセンティブを授受する方法の例として、ＩＣカード３４０１が持っている有価値情報（例えば金銭と同等または類似の情報、ユーザの個人情報や利用度数情報など）を利用機３４０２に渡す、あるいは利用機３４０２が持っている情報（例えば広告情報、優待情報など）をＩＣカード３４０１に渡し、それをＩＣカード３４０１のユーザが閲覧したり取得することで利用機３４０２の所有者、運用者が直接的、間接的な意義を得ることが考えられる。なお、ＩＣカードのユーザ側においても何らかの利益を得るような仕組についても適宜利用可能である。これにより、利用機３３０２を設置、運用する人間あるいは組織に対してその見返りを与えることが可能となり、その実用的効果は大きい。

【０２２９】［第３５実施形態］第３５実施形態は前述した第３４実施形態のインセンティブ授受に関する第１の例であり、ＩＣカードシステムの構成は図３４と同様である。第３５実施形態では、インセンティブとして商業広告を用いる。即ち、ＩＣカード３４０１のインセンティブ発行手段３４０７は、利用機３４０２のインセンティブ獲得手段３４０８から、商業広告に関わる情報を受け取る。そして、ＩＣカード３４０１のユーザがこの情報を見ることにより商業広告効果が生じ、利用機３４０２の所有者もしくは運用者が、直接的もしくは間接的に商業広告収入を得ることが可能となる。

【０２３０】［第３６実施形態］第３６実施形態は前述した第３４実施形態のインセンティブ授受に関する第２の例であり、ＩＣカードシステムの構成は図３４と同様である。第３６実施形態では、インセンティブとして金銭もしくはその他の有価値情報を用いる。例えば金銭を用いた場合は、ＩＣカード３４０１のインセンティブ発行手段３４０７は、利用機３４０２のインセンティブ獲得手段３４０８に対し電子化された情報の授受により金銭支払いを行う。金銭以外の有価値物についても同様である。これにより、利用機３４０２の所有者もしくは運用者は、より直接的な利益を得ることが可能となる。

【０２３１】［その他の実施形態］本発明に係るＩＣカードシステムは、上述した実施形態に限定されるものではなく、構成や手順に関して種々の追加、変更が可能である。以下にその他の実施形態としていくつかの例を示す。

【０２３２】上述の第１～第３６実施形態において、構成装置であるＩＣカードを、ＩＣカードに類似したアーキテクチャを持つＩＣタグに置き換えた構成とすることも可能である。ＩＣタグは演算処理及び利用機との通信を行うことができる点においてＩＣカードに類似するが、その外形特徴はボタン型、札型、シール型、もしくは装身具に埋め込んだもの等、様々な形態にて実施し得る。

【０２３３】また、上述の実施形態において、構成装置であるＩＣカードを、携帯電話を含む携帯型情報端末に

置き換えた構成とすることも可能である。ただし、携帯型情報端末は電波、赤外線、接触端子等の手段を用いて利用機と直接通信を行うことが可能であることが条件である。

【０２３４】また、上述の実施形態において、構成装置であるＩＣカードを、マイコン内蔵メモリカードに置き換えた構成とすることも可能である。マイコン内蔵メモリカードは、比較的大容量の半導体メモリを持つカード型記憶媒体に、ＩＣカードと同様の処理能力と、利用機との通信機能とを付加した装置である。なお、大容量メモリカードとＩＣカードとを、他の機器で接続したものを用いた場合でも同様に実施可能である。

【０２３５】さらに、上述の実施形態において、構成装置である利用機を、街頭、店舗、駅、公共施設、学校、図書館等の不特定多数の人間が訪れる場所に設置する公共端末を用いた構成とすることも可能である。このような利用機が設置された施設を訪れる人間は、これに対応するＩＣカードを持参することで本発明が示す種々のサービスを享受できる。

【０２３６】また、上述の実施形態において、構成装置である利用機を、遊園地、博物館、イベント施設等の不特定多数の人間が訪れる場所で、レンタル品として貸し出される携帯電話機もしくは携帯型情報通信端末を用いた構成とすることも可能である。これにより、このような利用機を貸し出す施設を訪れる人間は、これに対応するＩＣカードを持参することで本発明が示す種々のサービスを享受できる。

【０２３７】また、上述の実施形態において、構成装置である利用機を、レンタカーに備え付けられるカーナビゲーション装置（自車の現在位置を地図上に表示したり、目的地までの道案内をする装置）を用いた構成とすることも可能である。なお、レンタカーに備え付けのものではなく、カーナビゲーション装置単体のレンタルでも良い。このようなカーナビゲーション装置の貸し出しを利用する人間は、これに対応するＩＣカードを持参することで本発明が示す種々のサービスを享受できる。

【０２３８】

【発明の効果】以上説明したように本発明によれば、第１に、ＩＣカード装置（ＩＣカード）とリモートホストとの間に設けられて両者とデータ通信を行い、ＩＣカード装置の代理として計算機ネットワーク上で機能するプロキシ装置（代理装置）を備え、さらにカード端末装置（利用機）が未知の変換アルゴリズムもしくは変換パラメータを用いてデータ変換を行うデータ変換手段を備えたことにより、ＩＣカードがプロキシ装置に渡したデータを、ＩＣカードユーザの意図通りに、かつ利用機ユーザにその結果を知られることなく、プロキシ装置内部において異なるデータに変化させることができる効果が得られる。

【０２３９】第２に、ＩＣカード装置内のアプリケーションがアクセスしようとするリモートホストのネットワーク上の位置及び通信方法に関わる情報を、プロキシ装置のデータ変換手段で生成したことにより、カード端末装置に対してアクセス先を隠蔽することができる効果が得られる。

【０２４０】第３に、ＩＣカード装置とプロキシ装置の二者間で暗号化に関するアルゴリズムと鍵情報を予め取り決め、この取り決めに基づいてカード端末装置に内容を知られることなく任意の情報をやりとりするセキュアパスを設けたことにより、ＩＣカード装置とプロキシ装置が通信する際に、中間に位置するカード端末装置に通信内容を隠蔽することができる効果が得られる。

【０２４１】第４に、上記セキュアパスを介してＩＣカード装置内におけるデータの暗号化手段を、アクセス先情報と転送データ情報について個別に備えたことにより、ＩＣカード装置がリモートホストに引き渡す転送データの内容を、カード端末装置だけでなくプロキシ装置にも隠蔽することができる効果が得られる。

【０２４２】第５に、ＩＣカード装置にはＵＩリクエスト情報送信手段を備え、プロキシ装置にＵＩリクエスト情報受信手段とＵＩ情報送信手段を備え、カード端末装置にＵＩ情報受信手段とＵＩ実行手段を備えたことにより、カード端末装置が持たないフォントの文字列情報等を表示することができる効果が得られる。

【０２４３】第６に、ＵＩ情報としてカード端末装置上に予め設けられた動作環境に適合するプログラムを用いたことにより、ＩＣカード装置が想定するＵＩが、カード端末装置の構成や仕様に強く依存せず独自のものとして実現可能となる効果が得られる。

【０２４４】第７に、ＩＣカード装置とプロキシ装置のどちらか片方もしくは両方に、カード端末装置の認証手段と評価手段を備えたことにより、ＩＣカード装置もしくはプロキシ装置が、カード端末装置の信頼度情報を獲得することができる効果が得られる。

【０２４５】第８に、ＩＣカード装置とプロキシ装置の両方にカード端末装置の評価手段を備え、片方が得た評価結果をセキュアパスを通じて他方に渡すようにしたことにより、ＩＣカード装置もしくはプロキシ装置のいずれか片方がカード端末装置の信頼度を獲得できた場合、もう一方にその情報を渡すことができる効果が得られる。また、両方が個別にカード端末装置の信頼度を獲得した場合は、それぞれの評価結果を違いに確認し合うことにより信頼度評価をより確実にすることができる効果が得られる。

【０２４６】第９に、ＩＣカード装置に送信情報制御手段を備えたことにより、ＩＣカード装置からカード端末装置に送信する情報内容をカード端末装置の信頼度に従って異なるものにすることができる効果が得られる。さらに、ＩＣカード装置が機密情報として保持する情報をカード端末装置に送信しないよう送信情報制御手段を作

用させることにより、個人情報等をカード端末装置毎の信頼度に応じて管理することができる効果が得られる。

【０２４７】第１０に、プロキシ装置に送信情報制御手段を備えたことにより、プロキシ装置からカード端末装置に送信する情報内容を、上記のＩＣカード装置の場合と同様にカード端末装置の信頼度によって異なるものにでき、信頼度の低いカード端末装置には機密情報を渡さないといったセキュリティ管理を行うことができる効果が得られる。

【０２４８】第１１に、プロキシ装置上において、上記のＵＩ情報送信手段に、上記の送信情報制御手段を連動させ、カード端末装置の評価結果に従ってプロキシ装置からカード端末装置に送信するＵＩ情報に対して変更、削除、追加等の処理を行うようにしたことにより、信頼度の低いカード端末装置を使用する場合、機密情報をカード端末装置の画面上に表示してそれを取得されて漏洩してしまったり、また暗証番号等を不用意に入力して取得されてしまうなどのトラブルを防止することができる効果が得られる。

【０２４９】第１２に、ＩＣカード装置もしくはプロキシ装置に機密情報変換手段を設け、ユーザがカード端末装置に入力した仮の機密情報を、機密情報変換手段が真の機密情報に変換することで、暗証番号、パスワード等の機密情報をカード端末装置に秘匿した状態でリモートホストに渡し、リモートホストのサービスを受けられるようになる効果が得られる。

【０２５０】第１３に、ＩＣカード装置にプロキシ選択手段を備えたことにより、ＩＣカード装置毎、カード端末装置毎等に持つ条件に従って異なるプロキシ装置が利用可能となり、ネットワーク負荷及びプロキシの処理負荷の集中緩和を図ることができる効果が得られる。

【０２５１】第１４に、ＩＣカード装置にインセンティブ発行手段を備え、カード端末装置にインセンティブ獲得手段を備えたことにより、カード端末装置の所有者、運営者が直接的もしくは間接的利益を獲得することができる効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図２】本発明の第２実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図３】第２実施形態におけるアクセス先情報及び通信キーデータの関係を例示した動作説明図。

【図４】第２実施形態におけるアクセス先秘匿処理の流れを示したフローチャート。

【図５】本発明の第３実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図６】本発明の第５実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図７】本発明の第９実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図８】第９実施形態におけるＵＩ制御処理の流れを示したフローチャート。

【図９】第９実施形態のＩＣカードシステムにおけるＵＩリクエスト情報及びＵＩ情報のデータ構造、並びにＵＩ実行結果の一例を示す動作説明図。

【図１０】本発明の第１３実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図１１】第１３実施形態における利用機の信頼度評価処理の流れを示したフローチャート。

【図１２】本発明の第１４実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図１３】第１４実施形態における利用機の信頼度評価処理の流れを示したフローチャート。

【図１４】本発明の第１６実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図１５】本発明の第２０実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図１６】本発明の第２４実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図１７】第２４実施形態におけるＵＩ実行処理の流れを示したフローチャート。

【図１８】第２４実施形態におけるＵＩリクエスト情報の一例を示す動作説明図。

【図１９】第２４実施形態におけるＵＩ情報及びＵＩ実行結果の第１の例を示す動作説明図。

【図２０】第２４実施形態におけるＵＩ情報及びＵＩ実行結果の第２の例を示す動作説明図。

【図２１】第２４実施形態におけるＵＩ情報及びＵＩ実行結果の第３の例を示す動作説明図。

【図２２】本発明の第２５実施形態にＵＩリクエスト情報及びＵＩ実行結果の例を示す動作説明図。

【図２３】第２５実施形態におけるＵＩ実行結果の具体例を示す動作説明図。

【図２４】第２５実施形態におけるＵＩ実行結果の具体例を示す動作説明図。

【図２５】本発明の第２６実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図２６】第２６実施形態における機密情報保護処理の流れを示したフローチャート。

【図２７】第２６実施形態におけるＵＩ実行結果とリモートホストに渡されるデータの具体例を示した動作説明図。

【図２８】第２７実施形態におけるＵＩ実行結果の具体例を示す動作説明図。

【図２９】第２８実施形態におけるＵＩ実行結果の具体例を示す動作説明図。

【図３０】本発明の第２９実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図３１】本発明の第３０実施形態に係るプロキシ選択

動作の概念を示す説明図。

【図３２】本発明の第３１実施形態に係るプロキシ選択動作の概念を示す説明図。

【図３３】本発明の第３３実施形態に係るプロキシ情報操作機能を有するＩＣカードを示す説明図。

【図３４】本発明の第３４実施形態に係るＩＣカードシステムの構成を示すブロック図。

【図３５】従来のＩＣカードシステムの構成例を示すブロック図。

【符号の説明】

１０１　ＩＣカード

＊１０２　利用機

１０３　プロキシ装置

１０４　リモートホスト

１０５　計算機ネットワーク

１０６　送信用データ保持手段

１０７　データ送信手段

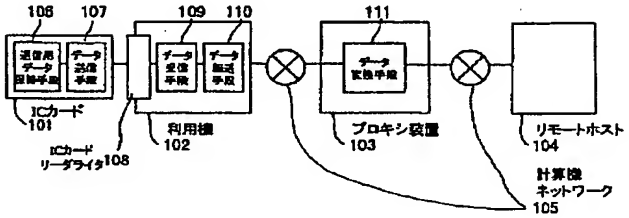
１０８　ＩＣカードリーダライタ

１０９　データ受信手段

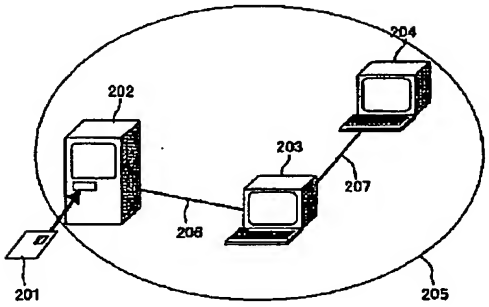
１１０　データ転送手段

１１１　データ変換手段

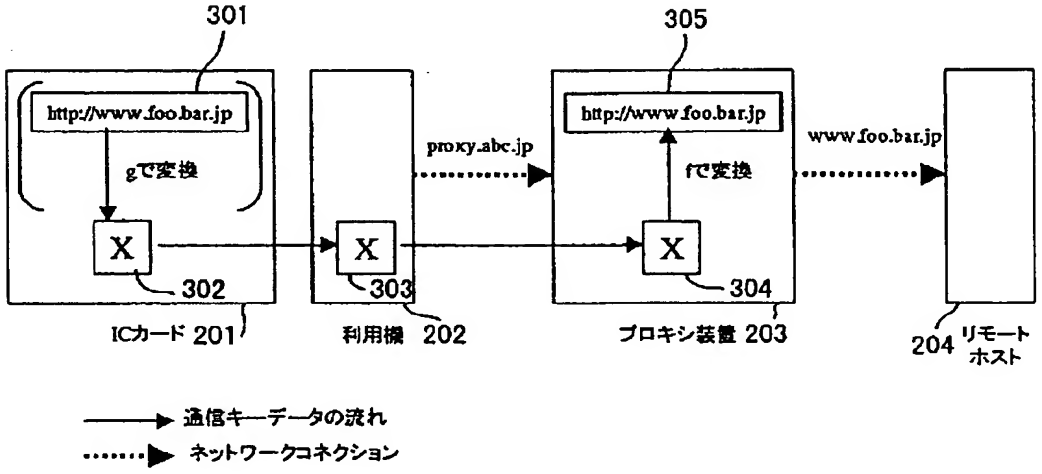
【図１】



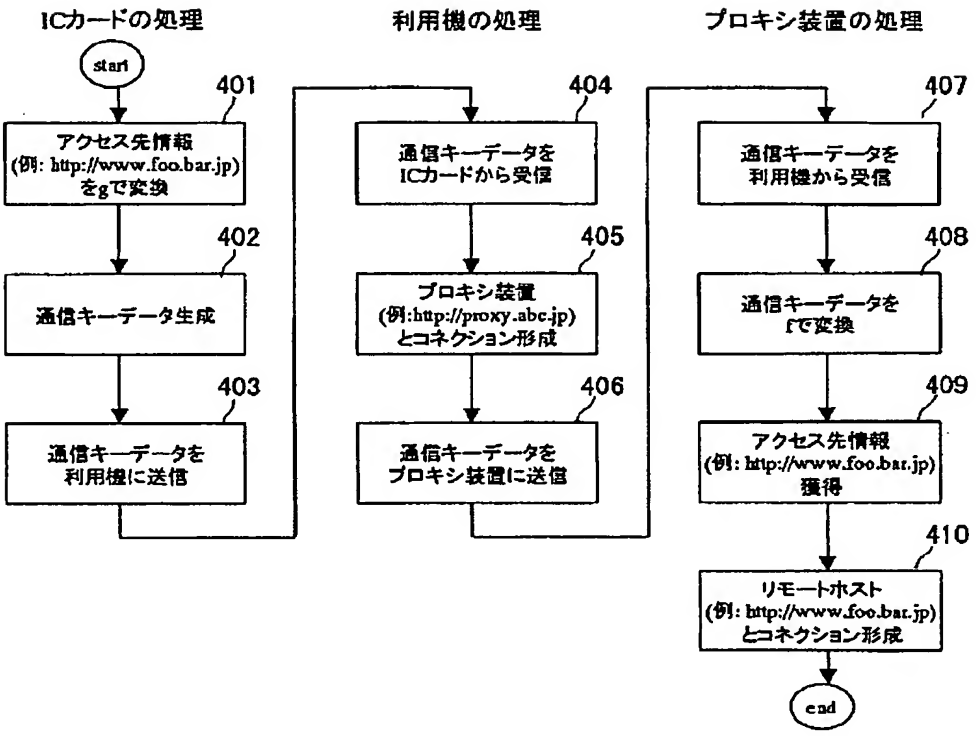
【図２】



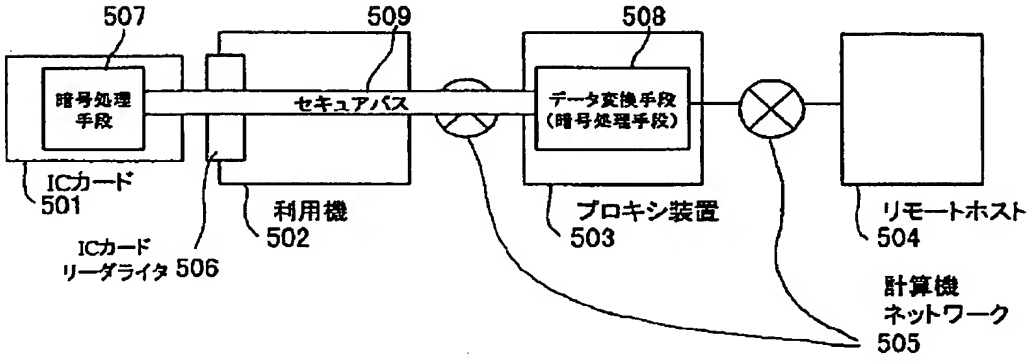
【図３】



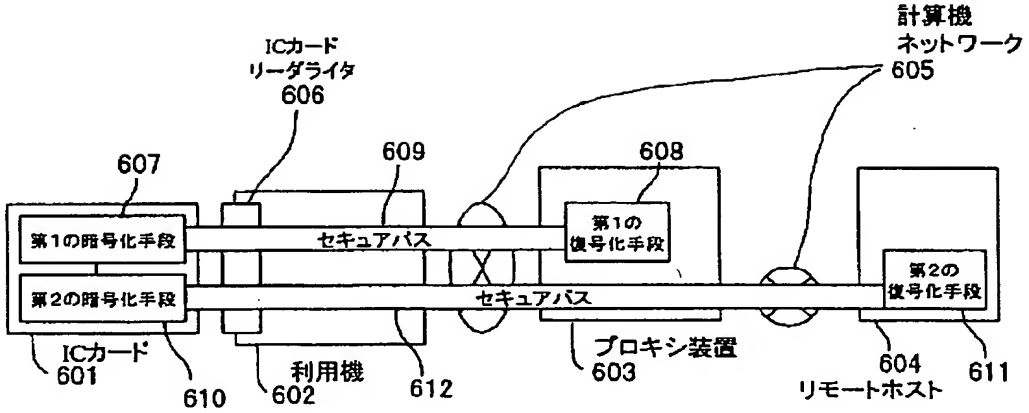
【図４】


ICカードの処理
利用機の処理
プロキシ装置の処理
start
401
アクセス先情報
(例: http://www.foo.bar.jp)
をgで変換
402
通信キーデータ生成
403
通信キーデータを
利用機に送信
404
通信キーデータを
ICカードから受信
405
プロキシ装置
(例:http://proxy.abc.jp)
とコネクション形成
406
通信キーデータを
プロキシ装置に送信
407
通信キーデータを
利用機から受信
408
通信キーデータを
fで変換
409
アクセス先情報
(例: http://www.foo.bar.jp)
獲得
410
リモートホスト
(例: http://www.foo.bar.jp)
とコネクション形成
end

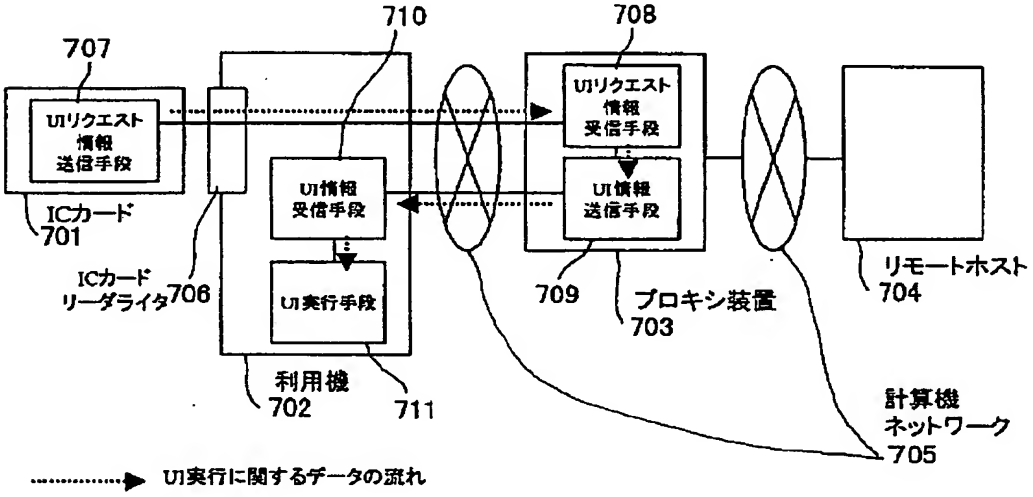
【図５】


507
509
508
暗号処理
手段
セキュアパス
データ変換手段
(暗号処理手段)
ICカード
501
利用機
502
プロキシ装置
503
リモートホスト
504
ICカード
リーダライタ 506
計算機
ネットワーク
505

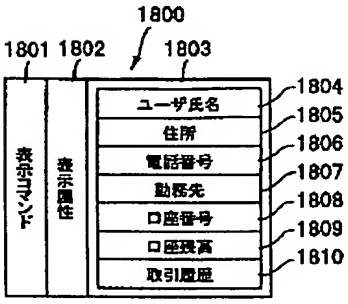
【図６】


計算機
ネットワーク
605
ICカード
リーダライタ
606
607
609
608
第1の暗号化手段
セキュアパス
第1の
復号化手段
第2の暗号化手段
セキュアパス
第2の
復号化手段
ICカード
601
610
利用機
602
612
プロキシ装置
603
604
リモートホスト
611

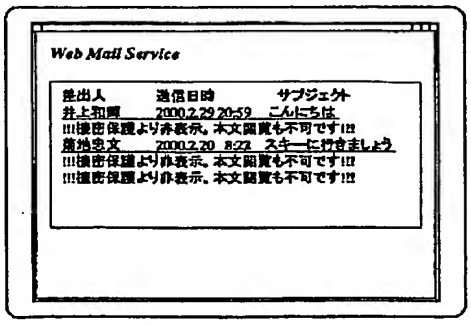
【図７】


710
708
707
UIリクエスト
情報
送信手段
UIリクエスト
情報
受信手段
UI情報
受信手段
UI情報
送信手段
ICカード
701
ICカード
リーダライタ
706
UI実行手段
709
プロキシ装置
703
リモートホスト
704
利用機
702
711
計算機
ネットワーク
705
UI実行に関するデータの流れ

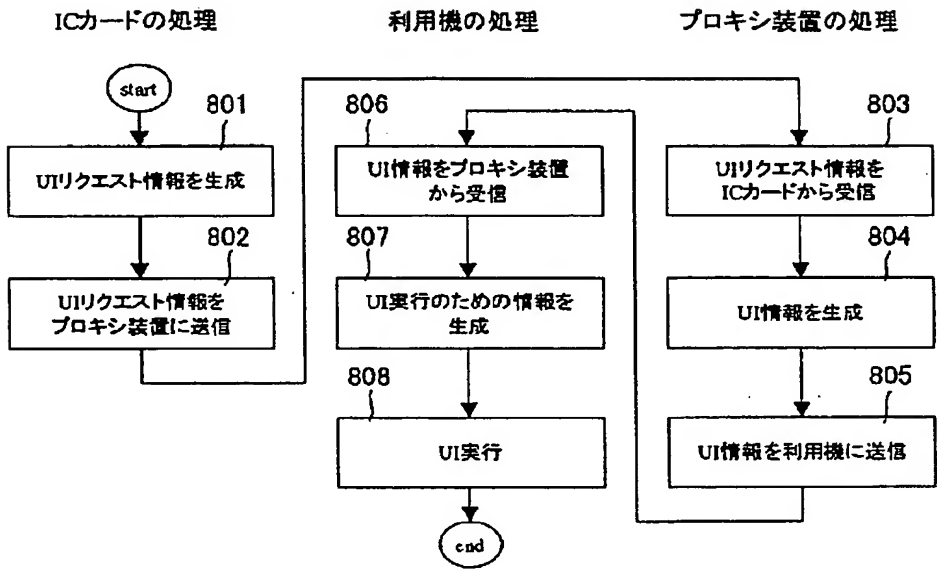
【図１８】


1800
1801
1802
1803
表示コマンド
表示属性
ユーザ氏名
住所
電話番号
勤務先
口座番号
口座残高
取引履歴
1804
1805
1806
1807
1808
1809
1810

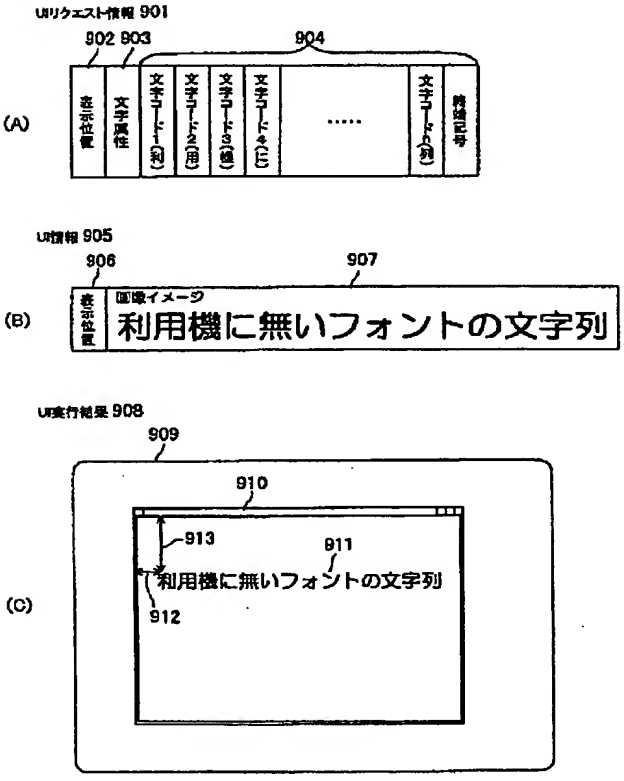
【図２４】


Web Mail Service
差出人
送信日時
サブジェクト
井上和輝
2000.2.29 20:59
こんにちは
!!!機密保護より非表示。本文閲覧も不可です!!!
原地幸文
2000.2.20 8:23
スキーに行きましょう
!!!機密保護より非表示。本文閲覧も不可です!!!
!!!機密保護より非表示。本文閲覧も不可です!!!

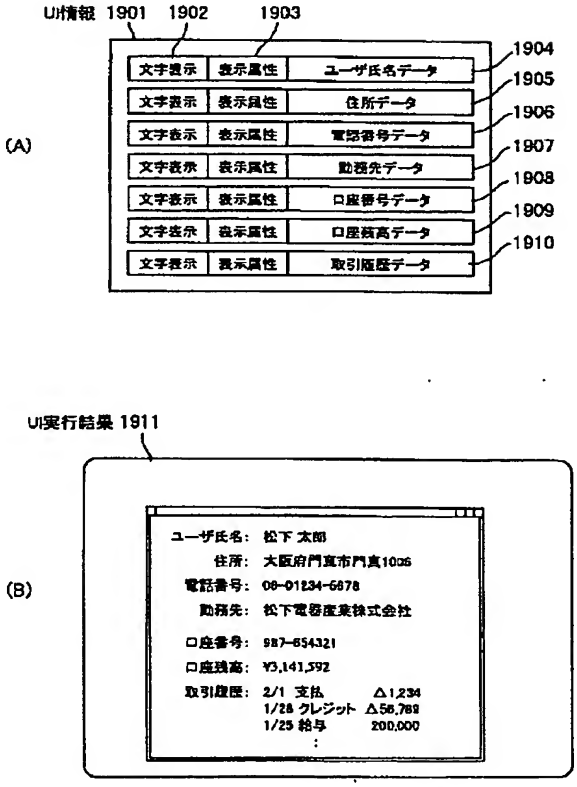
【図８】


ICカードの処理
利用機の処理
プロキシ装置の処理
start
801
UIリクエスト情報を生成
802
UIリクエスト情報を
プロキシ装置に送信
806
UI情報をプロキシ装置
から受信
807
UI実行のための情報を
生成
808
UI実行
end
803
UIリクエスト情報を
ICカードから受信
804
UI情報を生成
805
UI情報を利用機に送信

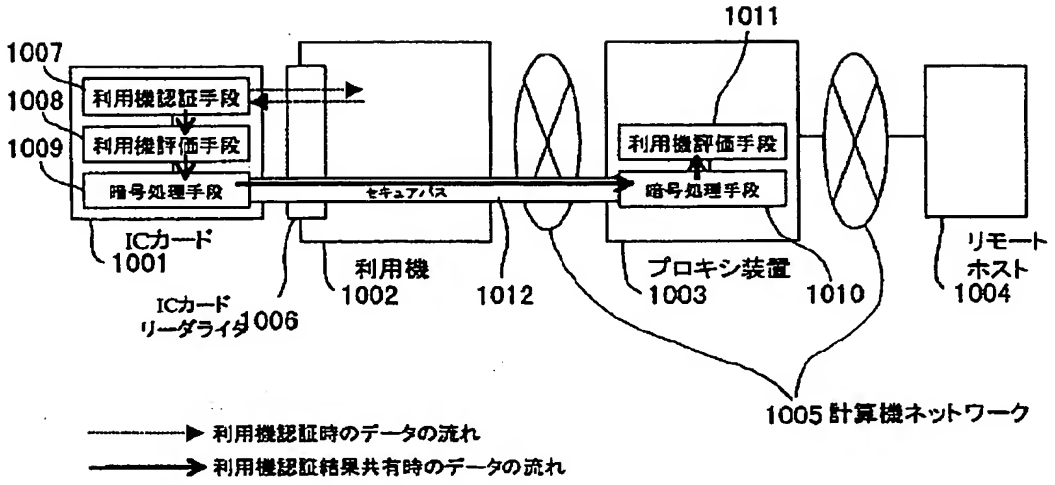
【図９】


UIリクエスト情報 901
902 903
904
(A)
表示位置
文字属性
文字コード1(利)
文字コード2(用)
文字コード3(機)
文字コード4(に)
.....
文字コードn(列)
終端記号
UI情報 905
906
907
(B)
表示位置
画像イメージ
利用機に無いフォントの文字列
UI実行結果 908
909
910
913
911
(C)
利用機に無いフォントの文字列
912

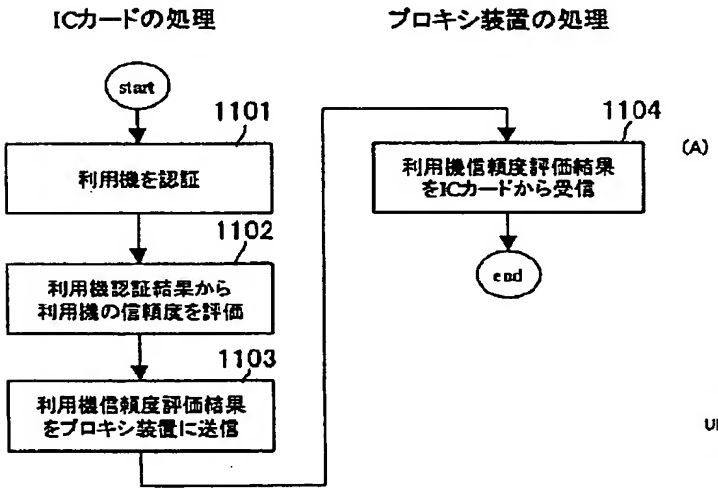
【図１９】


UI情報 1901 1902 1903
(A)
文字表示 表示属性 ユーザ氏名データ 1904
文字表示 表示属性 住所データ 1905
文字表示 表示属性 電話番号データ 1906
文字表示 表示属性 勤務先データ 1907
文字表示 表示属性 口座番号データ 1908
文字表示 表示属性 口座残高データ 1909
文字表示 表示属性 取引履歴データ 1910
UI実行結果 1911
(B)
ユーザ氏名: 松下 太郎
住所: 大阪府門真市門真1006
電話番号: 06-01234-6678
勤務先: 松下電器産業株式会社
口座番号: 987-654321
口座残高: ¥3,141,592
取引履歴: 2/1 支払 △1,234
1/28 クレジット △56,789
1/25 給与 200,000

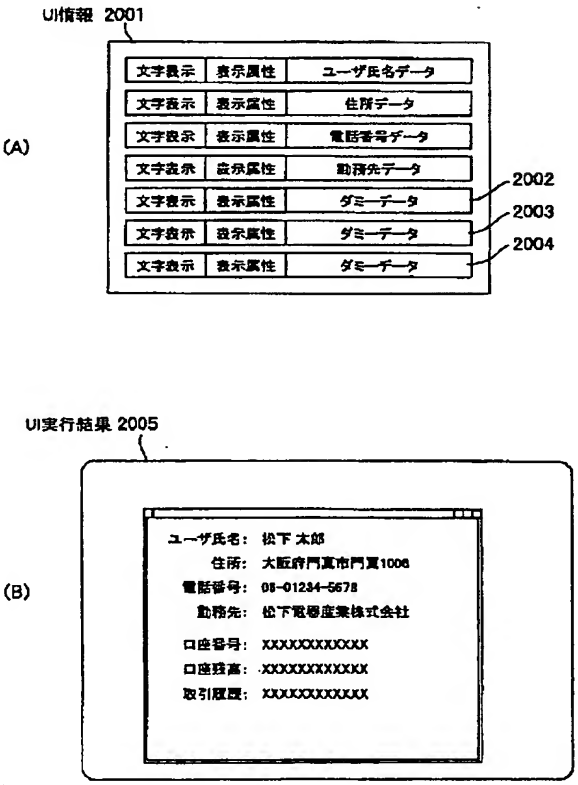
【図１０】



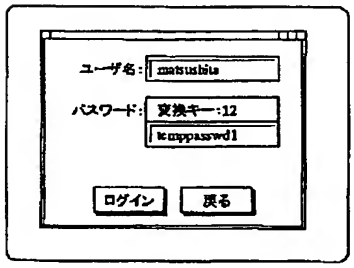
【図１１】



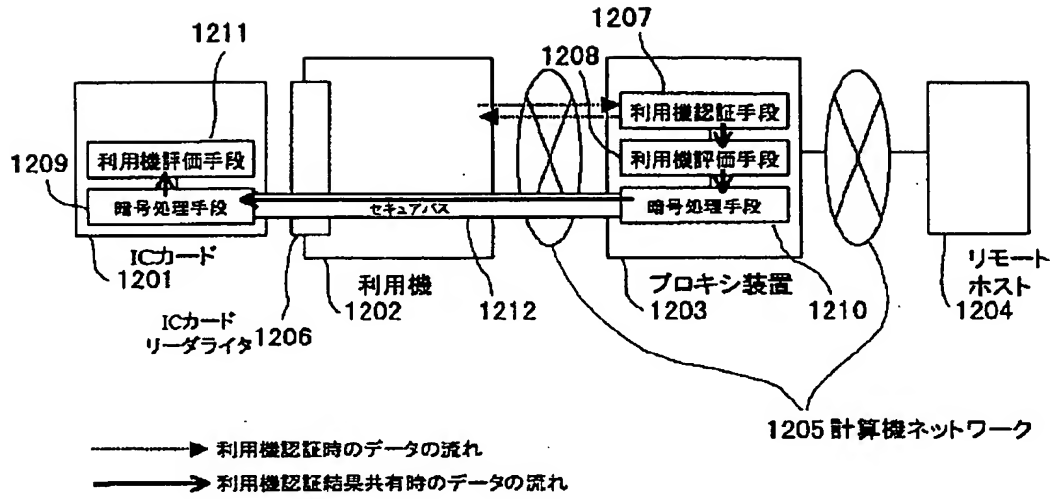
【図２０】



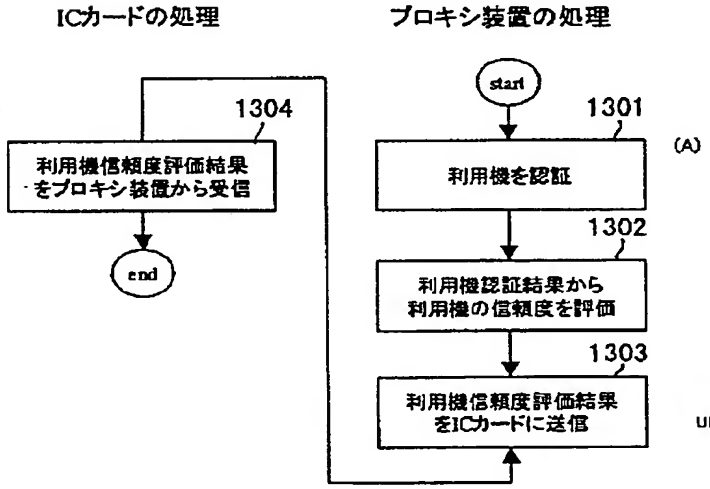
【図２８】



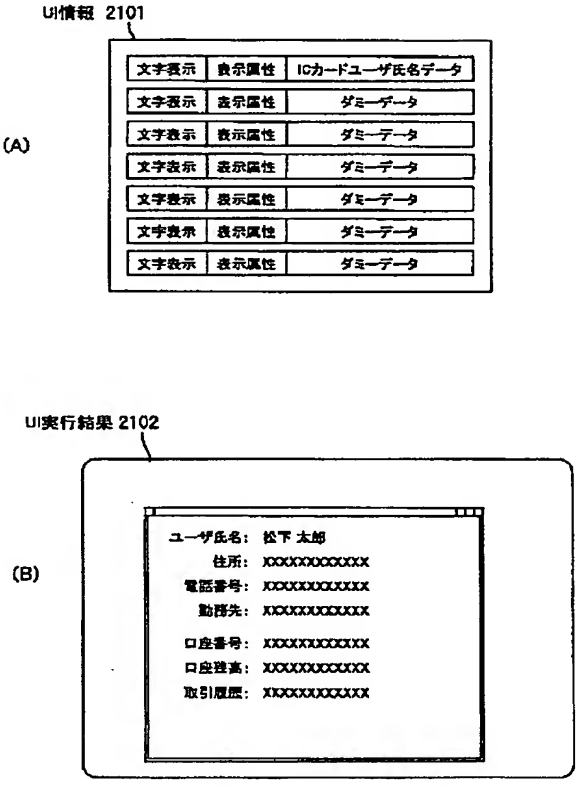
【図１２】



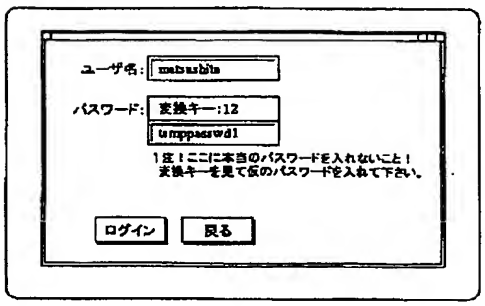
【図１３】



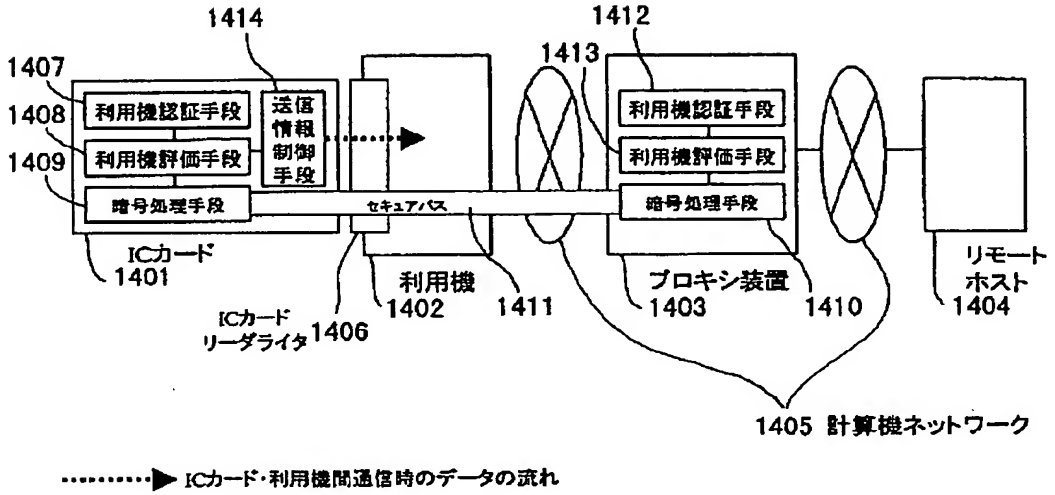
【図２１】



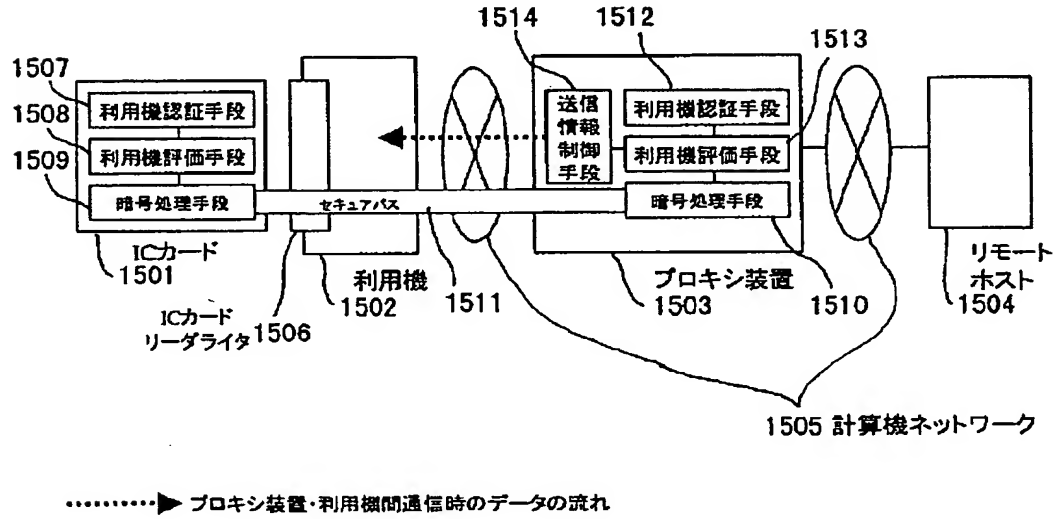
【図２９】



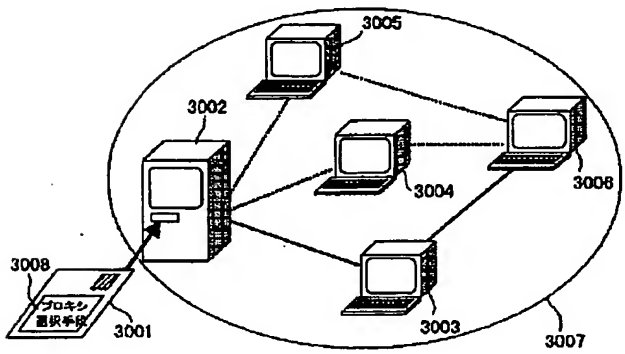
【図１４】



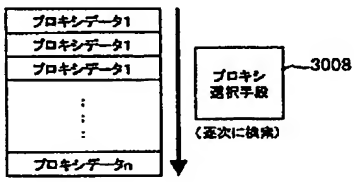
【図１５】



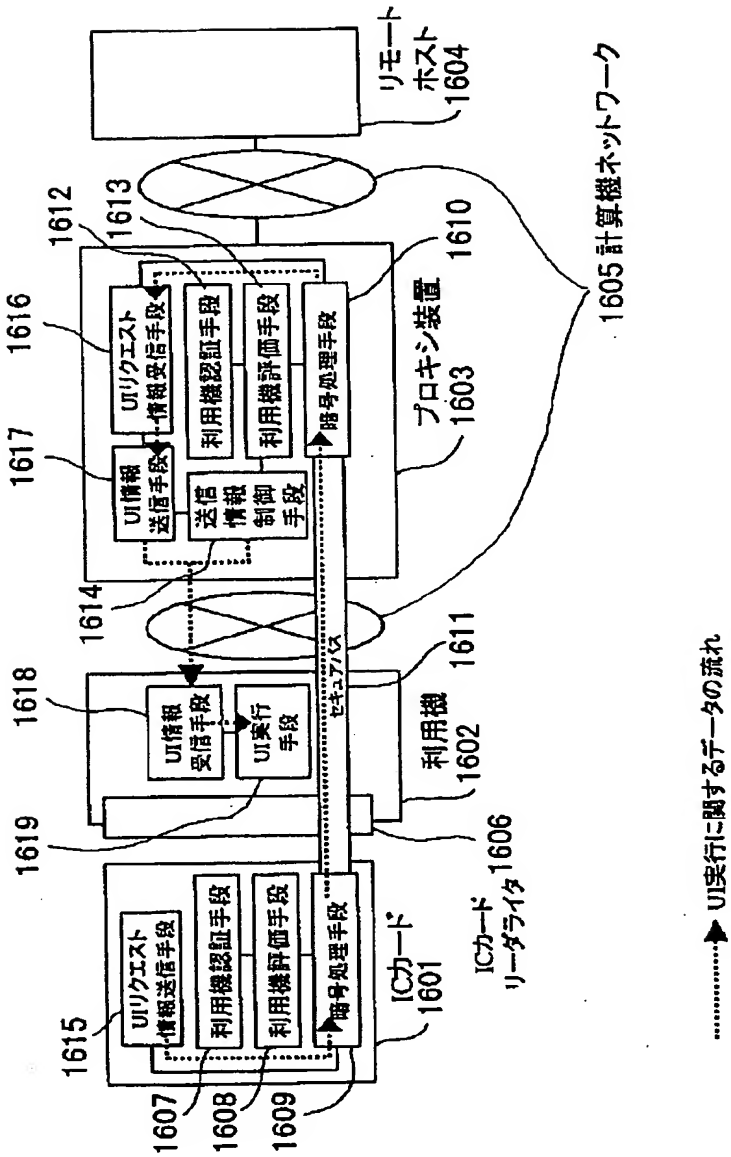
【図３０】



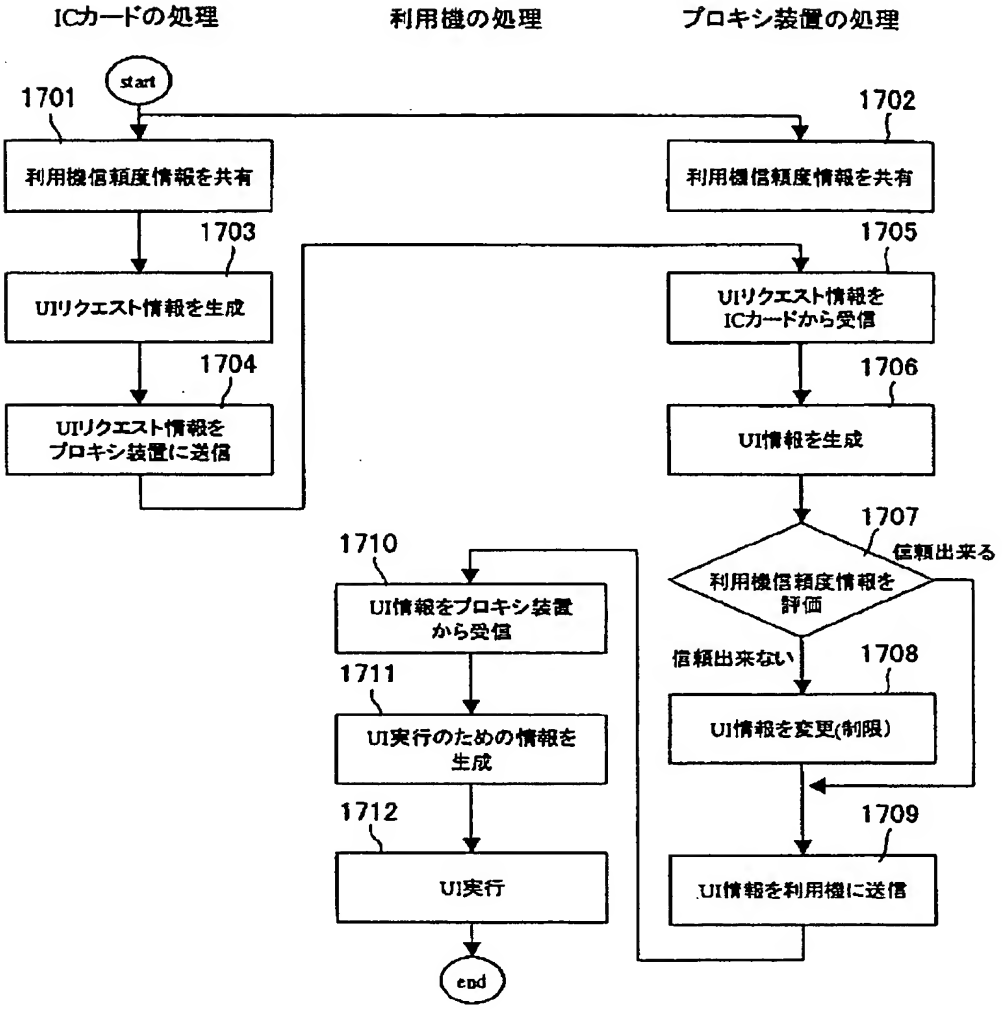
【図３１】



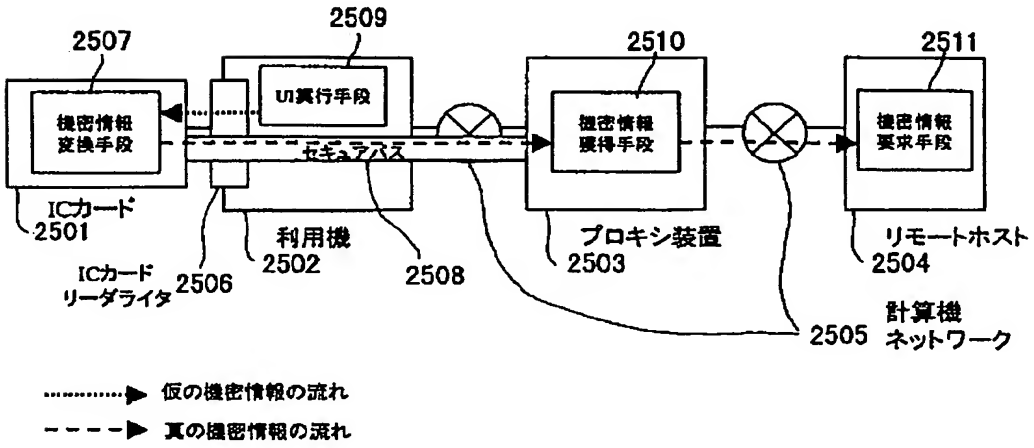
【図１６】


リモートホスト
1604
1605 計算機ネットワーク
プロキシ装置
1603
1610
1612
1613
1616
1617
1614
1618
1619
1611
利用機
1602
ICカード
リーダライタ1606
ICカード
1601
1615
1607
1608
1609
UIリクエスト情報送信手段
利用機認証手段
利用機評価手段
暗号処理手段
UI情報送信手段
送信情報制御手段
UIリクエスト情報受信手段
UI情報受信手段
UI実行手段
セキュアバス
UI実行に関するデータの流れ

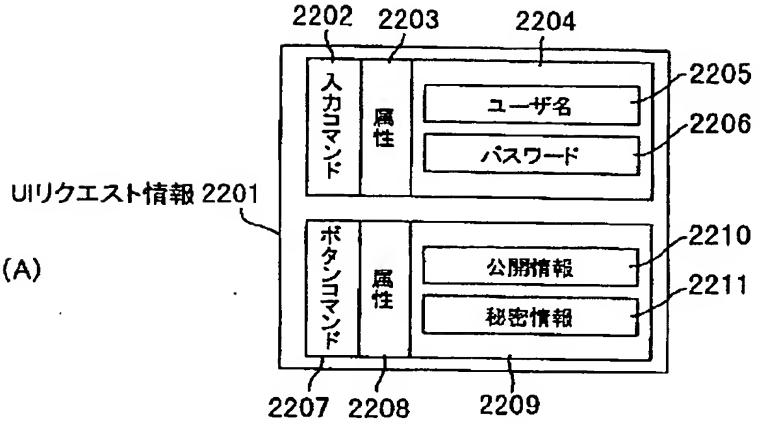
【図１７】

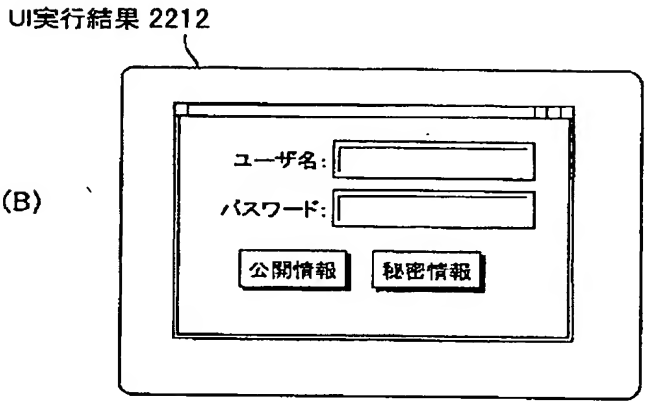

ICカードの処理
利用機の処理
プロキシ装置の処理
start
1701
利用機信頼度情報を共有
1702
利用機信頼度情報を共有
1703
UIリクエスト情報を生成
1704
UIリクエスト情報を
プロキシ装置に送信
1705
UIリクエスト情報を
ICカードから受信
1706
UI情報を生成
1707
信頼出来る
利用機信頼度情報を
評価
信頼出来ない
1708
UI情報を変更(制限)
1709
UI情報を利用機に送信
1710
UI情報をプロキシ装置
から受信
1711
UI実行のための情報を
生成
1712
UI実行
end

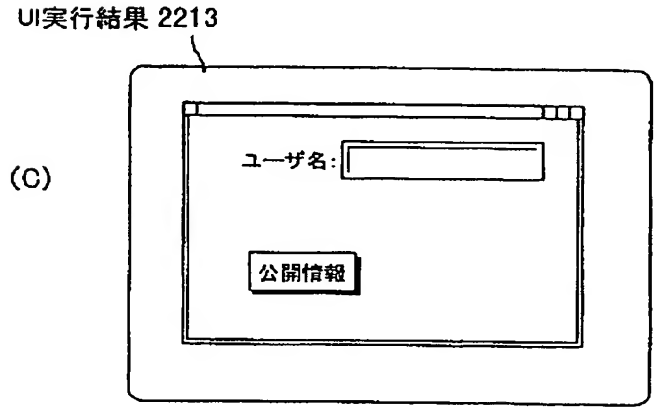
【図２５】


2507
機密情報
変換手段
ICカード
2501
2509
UI実行手段
セキュアパス
利用機
2502
2506
ICカード
リーダライタ
2508
2510
機密情報
獲得手段
プロキシ装置
2503
2511
機密情報
要求手段
リモートホスト
2504
2505
計算機
ネットワーク
仮の機密情報の流れ
真の機密情報の流れ

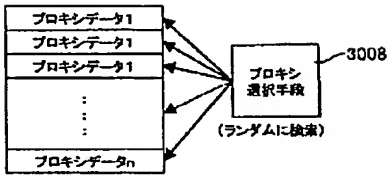
【図２２】


2202
2203
2204
入力コマンド
属性
ユーザ名
パスワード
2205
2206
UIリクエスト情報 2201
(A)
ボタンコマンド
属性
公開情報
秘密情報
2210
2211
2207
2208
2209

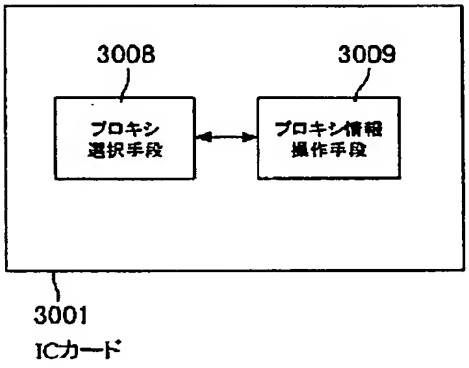

UI実行結果 2212
(B)
ユーザ名:
パスワード:
公開情報
秘密情報


UI実行結果 2213
(C)
ユーザ名:
公開情報

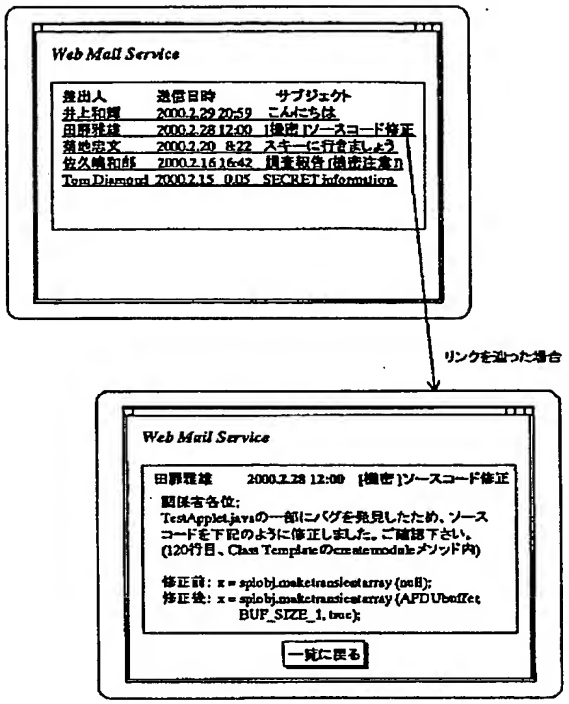
【図３２】


プロキシデータ1
プロキシデータ1
プロキシデータ1
プロキシデータn
プロキシ選択手段
3008
(ランダムに検索)

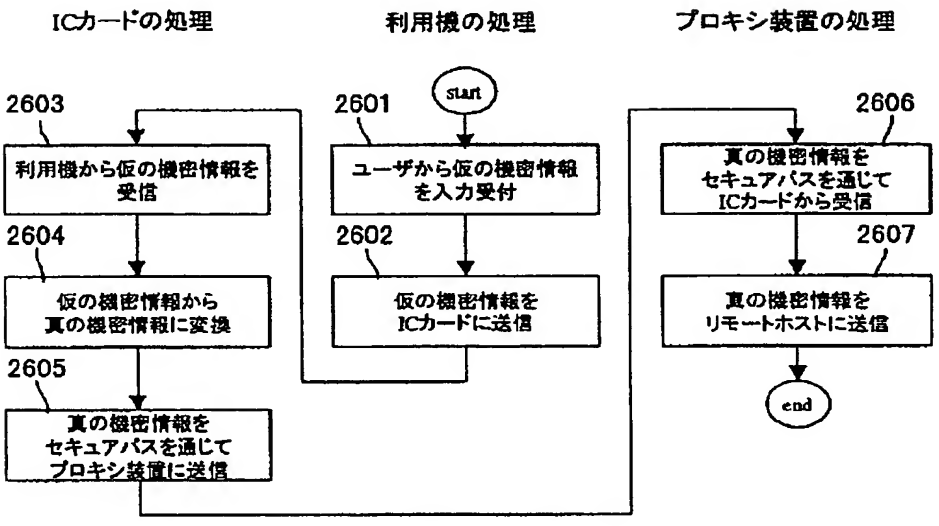
【図３３】


3008
3009
プロキシ選択手段
プロキシ情報操作手段
3001
ICカード

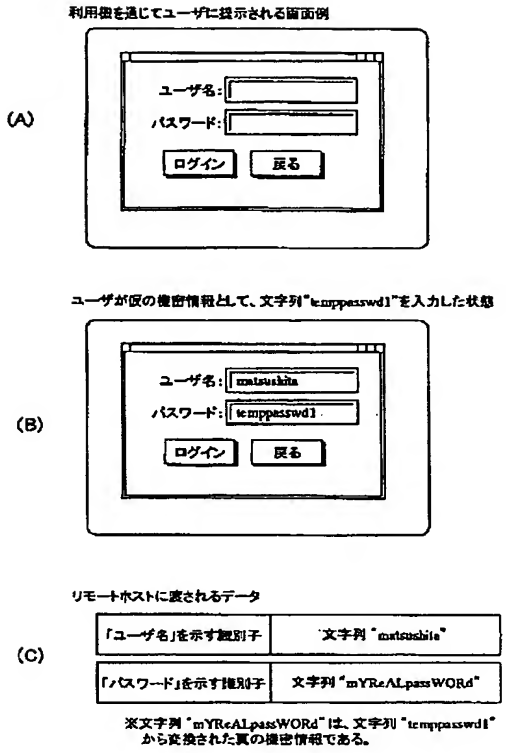
【図２３】


Web Mail Service
差出人 送信日時 サブジェクト
井上和輝 2000.2.29 20:59 こんにちは
田野雅雄 2000.2.28 12:00 [機密]ソースコード修正
荒地宏文 2000.2.20 8:22 スキーに行きましょう
佐久晴和郎 2000.2.16 16:42 関東報告(機密注意)
Tom Diamond 2000.2.15 0:05 SECRET information
リンクを辿った場合
Web Mail Service
田野雅雄 2000.2.28 12:00 [機密]ソースコード修正
関係各位:
TestApplet.javaの一部にバグを発見したため、ソースコードを下記のように修正しました。ご確認下さい。
(120行目、Class Templateのcreatemoduleメソッド内)
修正前: x = spiobj.maketransientarray (ocll);
修正後: x = spiobj.maketransientarray (APDUbuffer, BUF_SIZE_1, true);
一覧に戻る

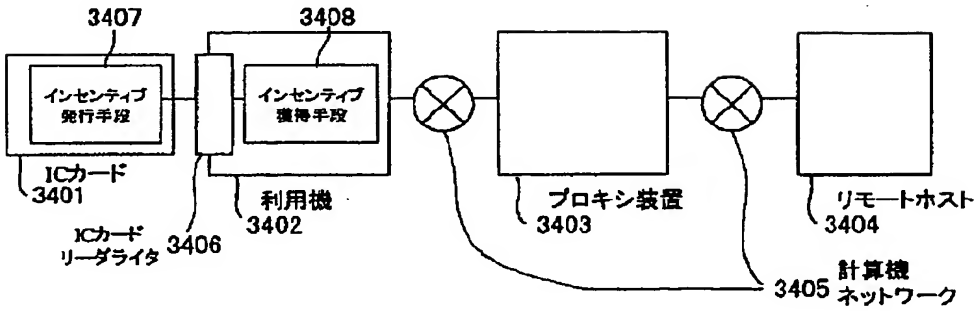
【図２６】


ICカードの処理
利用機の処理
プロキシ装置の処理
start
2601
ユーザから仮の機密情報を入力受付
2602
仮の機密情報をICカードに送信
2603
利用機から仮の機密情報を受信
2604
仮の機密情報から真の機密情報に変換
2605
真の機密情報をセキュアパスを通じてプロキシ装置に送信
2606
真の機密情報をセキュアパスを通じてICカードから受信
2607
真の機密情報をリモートホストに送信
end

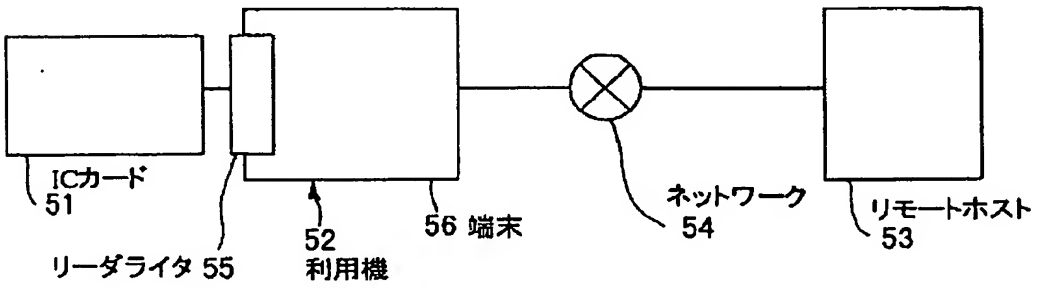
【図２７】


利用機を通じてユーザに提示される画面例
(A)
ユーザ名:
パスワード:
ログイン
戻る
ユーザが仮の機密情報として、文字列"tcmppasswd1"を入力した状態
(B)
ユーザ名: matsushita
パスワード: tcmppasswd1
ログイン
戻る
リモートホストに渡されるデータ
(C)
「ユーザ名」を示す識別子
文字列 "matsushita"
「パスワード」を示す識別子
文字列 "mYReALpassWORd"
※文字列 "mYReALpassWORd" は、文字列 "tcmppasswd1" から変換された真の機密情報である。

【図３４】


3407
3408
インセンティブ発行手段
インセンティブ獲得手段
ICカード
3401
ICカード
リーダライタ
3406
利用機
3402
プロキシ装置
3403
リモートホスト
3404
3405
計算機
ネットワーク

【図３５】


ICカード
51
リーダライタ 55
52
利用機
56 端末
ネットワーク
54
リモートホスト
53

フロントページの続き

(72)発明者　田靡　雅基
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　菊地　隆文
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　2C005 MB03 MB05 MB10 SA02 SA12 SA25 TA27 TA28
5B035 AA13 BB09 BC00 CA29
5B058 CA23 KA02 KA04 YA20
5B085 AE12 AE29
5J104 AA01 NA02 NA35 NA37 NA40 PA07